T-Com

Speedport 400P
Bedienungsanleitung

Sicherheitshinweise

Beachten Sie die folgenden Hinweise um sich vor körperlichen Schäden zu bewahren:

- Verlegen Sie die Anschluss-Schnüre unfallsicher! Es dürfen keine Stolperfallen entstehen!
- Niemals
  – das Gerät selbst öffnen!
  – Steckkontakte mit spitzen und metallischen Gegenständen berühren!
- Den Speedport 400P nur mit dem mitgeliefertem Netzteil betreiben. Das Netzteil nicht mit nassen Händen anfassen. Nur an Stromsteckdosen anschließen, die den im Typenschild angegebenen Werten entsprechen.

Beachten Sie beim Aufstellen, Anschließen und Bedienen des Speedport 400P unbedingt die folgenden Hinweise:

- Bei Auf-Tisch-Betrieb: Stellen Sie das Gerät auf eine rutschfeste Unterlage!
- Achten Sie darauf, dass die Lüftungsschlitze nie verdeckt werden! Legen Sie keine Gegenstände darauf ab.
- Bei Wandmontage: Achten Sie darauf, dass Sie beim Bohren der Dübellöcher keine in der Wand verlaufenden Leitungen oder Rohre treffen.
- Stellen Sie das Gerät entfernt von
  – Wärmequellen,
  – direkter Sonneneinstrahlung,
  – anderen elektrischen Geräten auf.
- Schützen Sie das Gerät vor Nässe, Staub, aggressiven Flüssigkeiten und Dämpfen.
- Schließen Sie die Anschluss-Schnüre nur an den dafür vorgesehenen Dosen an.
- Reinigen Sie das Gerät mit einem leicht feuchten, fusselfreien Tuch oder mit einem Antistatiktuch.
- Benutzen Sie das Gerät nicht in Feuchträumen (z. B. Bad) oder in explosionsgefährdeten Bereichen.
- Das Gerät darf nur vom autorisierten Service-Personal repariert werden.

- Eine Haftung der T-Com für Schäden aus nicht bestimmungsgemäßem Gebrauch des Speedport 400P kann nicht übernommen werden.

Das von Ihnen erworbene Produkt wird von T-Com auch weiterhin gepflegt. Unter http://www.t-com.de finden Sie auf der Startseite einen Link zu Faq & Downloads. Dort unter Software und Treiber den Link zu Downloads. Sie können das Produkt Speedport 400P wählen.

Hinweise

Dieses Zeichen warnt vor Gefahren. Bitte beachten Sie die Hinweise.

Dieses Zeichen weist Sie auf nützliche Hinweise und zusätzliche Informationen hin.

Das Ausrufezeichen markiert wichtige Informationen und Hinweise, die Sie auf jeden

Inhaltsverzeichnis

Sicherheitshinweise ... II
Hinweise ... III
Inhaltsverzeichnis ... V
Willkommen ... 1
Anschluss von einem oder mehreren Computern ... 1
Internetverbindung für alle Computer ... 1
Schutz durch integrierte Firewall ... 2
Gerät in Betrieb nehmen ... 3
Gerät auspacken ... 3
Verpackungsinhalt überprüfen ... 3
Aufstellungsort ... 4
Aufstellen des Speedport 400P ... 4
Wandmontage ... 4
Anschließen ... 5
Anschlüsse auf der Rückseite des Speedport 400P ... 5
Anzeigen ... 6
Speedport 400P an die Stromversorgung anschließen ... 7
Speedport 400P am DSL anschließen ... 8
Speedport 400P mit dem LAN Anschluss des Computers verbinden ... 8
ISDN-Anschluss (optional) ... 9
Konfiguration des Speedport 400P ... 10
Vorbereiten des einzubindenden Rechners/Netzwerkes ... 10
Prüfen der Netzanbindung der Ethernetkarte ... 10
Konfiguration des PCs unter Windows XP ... 11
Konfiguration des PCs unter Windows 2000 ... 13
Erstkonfiguration ... 15
Der Web-Konfigurator ... 15
Konfiguration mit dem Einrichtungsassistent ... 16
Einrichtungsassistent ... 19
Ausloggen ... 20
Im Internet surfen ... 21
Erweiterte Konfiguration ... 23
Status ... 24
Statusseite ... 24

ARP Tabelle 27
Routing Tabelle 28
Routing Tabelle 28
RIP Routing Tabelle 29
DHCP Tabelle 29
Leased Tabelle 30
Fristablauf Tabelle 30
Permanent Tabelle 30
PPTP Status 31
IPSec Status 32
L2TP Status 33
Email Status 34
Ereignis Protokoll 34
Fehler Protokoll 35
NAT Sitzungen 35
Diagnose 36
UPnP Portmap 37
Einrichtungsassistent 38
T-DSL Business mit dynamischer IP Adresse 40
Im Internet surfen 41
T-DSL Business mit fester IP Adresse 43
Im Internet surfen 44
Anderer Anbieter 46
Im Internet surfen 47
Konfiguration 50
LAN (Local Area Network) 51
Bridge Schnittstelle 51
Ethernet 52
Ethernet Client Filter 52
Port Einstellungen 54
DHCP Server 56
WAN (Wide Area Network) 58
ISP 58
RFC 1483 Routed Verbindungen 59
RFC 1483 Bridged Verbindungen 60
PPPoA Routed Verbindungen 62

IPoA Routed Verbindungen 66
PPPoE Verbindungen 67
Erweiterte Optionen (PPPoE) 69
PPPoE mit Pass-through Verbindungen 72
Erweiterte Optionen (PPPoE) 74
Backup ISP 76
DNS 77
ADSL 78
Erweiterte Optionen 80
System 81
Zeitzone 81
Remote Zugriff 82
Firmware Upgrade 82
Sichern / Wiederherstellen 83
Neustart 84
Benutzer Verwaltung 84
Firewall und Zugangskontrolle 86
Generelle Einstellungen 87
Paket Filter 89
Beispiel: Voreingestellte Paket Filter Regeln 89
Paket Filter –TCP/UDP Filter hinzufügen 91
Paket Filter – Raw IP Filter hinzufügen 92
Beispiel:
Konfiguration der Firewall für einen Zugriff vom Internet auf den Webserver des Router 93
Konfiguration Paket Filter: 94
Angriffserkennung 96
Blockierungsdauer: 97
URL Filter 99
Firewall Protokoll 102
VPN (Virtual Private Networks) 103
PPTP 103
PPTP Remote Zugriffs Verbindung 103
LAN zu LAN PPTP Verbindung 105
IPSec 108
Konfiguration einer IPSec VPN Verbindung 108
Lokal: 108

Remote: 109
Erweiterte Optionen 110
Lokale ID: 111
Remote ID: 111
L2TP 112
Remote Zugriffs L2TP Verbindung 113
LAN zu LAN L2TP Verbindung 116
Beispiele VPN Konfiguration 119
Beispiel:
Konfiguration einer Fernzugriff PPTP VPN Einwahlverbindung 119
Konfiguration PPTP VPN in der Firma 119
Beispiel:
Konfiguration einer Fernzugriff PPTP VPN Dial-out Verbindung 120
Konfiguration von PPTP VPN in der Firma 120
Beispiel:
Konfiguration einer LAN-zu-LAN PPTP VPN Verbindung 121
Konfiguration PPTP VPN in der Firma 122
Konfiguration PPTP VPN im Filialbüro 123
Beispiel: Konfiguration einer IPSec LAN-zu-LAN VPN Verbindung 124
Konfiguration von IPSec VPN im Hauptbüro 125
Konfiguration IPSec VPN in der Filiale 126
Beispiel:
Konfiguration einer IPSec Host-to-LAN VPN Verbindung 127
Konfiguration IPSec VPN im Hauptbüro 127
Beispiel:
Konfiguration eines Remote Access L2TP VPN Dial-in Verbindung 128
Konfiguration von L2TP VPN im Hauptbüro 129
Beispiel:
Konfiguration einer Remote Access L2TP VPN Dial-out Verbindung 130
Konfiguration von L2TP VPN im Firmenbüro 131
Beispiel: Konfiguration Ihres Routers zur Einwahl in den Server 132
Beispiel: Konfiguration einer LAN-zu-LAN L2TP VPN Verbindung 132
Konfiguration von L2TP VPN im Hauptbüro 133
Konfiguration von L2TP im Filialbüro 134
ISDN Einwahl 136
QoS (Quality of Service) 137
Priorisation 137

IP Throttling ausgehend (LAN zum WAN) 140
IP Throttling eingehend (WAN zum LAN) 142
Beispiel:
QoS für Ihr Netzwerk 143
Information und Einstellungen 144
Missionskritische Anwendungen 144
Sprach Anwendung 144
Limitierte Anwendungen 145
Erweiterte Einstellungen unter Verwendung von IP Throttling 145
Virtual Server (“Port Forwarding”) 147
Virtuellen Server hinzufügen 148
Beispiel:
Jederzeitiger Router-Zugriff per Fernwartung 149
DMZ Host bearbeiten 150
One-to-One NAT (Network Address Translation) bearbeiten 152
Beispiele: Liste einiger Well-Known und registrierten Port Nummern. . . . 154
Zeitplan 155
Konfiguration des Zeitplan 155
Zeitfenster bearbeiten 155
Löschen eines Zeitfenster 157
Erweitert 158
Statische Route 158
Dynamischer DNS 159
Prüfe Email 160
Geräte Management 162
Eingebauter Web Server 162
Universal Plug and Play (UPnP) 163
SNMP V1 und V2: 164
SNMP V3: 164
SNMP Version: SNMPv2c und SNMPv3 164
IGMP 166
VLAN Bridge 166
Beispiele für erweiterte VLAN Einstellungen (Triply Play) 167
Schritt 1: Einstellungen Mitglieder Ports 167
Schritt 2: Erstellen der WAN Schnittstelle 168
Schritt 3: VLAN Dienste einrichten 170
Schritt 4: IGMP Snooping Aktivieren 171

Speichern der Konfiguration im Flash 172
Ausloggen 172
Ratgeber 173
Weiterführende Hinweise 173
Was bei der Verkabelung zu beachten ist 173
Auslieferzustand 173
Problembehandlung 174
Fehler beim Öffnen der Benutzeroberfläche 174
LAN-Verbindung 174
IP-Einstellungen prüfen 174
IP-Einstellungen 174
Probleme beim Starten des Speedport 400P 175
Problem mit der WAN Schnittstelle 176
Problem mit der LAN Schnittstelle 176
Anhang 177
Technischer Kundendienst 177
Informationen und Updates 177
Unterstützung durch den Support 177
Gewährleistung für Speedport 400P 178
Technische Daten 179
Reinigen 179
CE-Konformitätserklärung 179
Recycling 180
Rücknahme von CD-ROM 180
Stichwortverzeichnis 181

Willkommen

Herzlichen Glückwunsch, dass Sie sich für den Speedport 400P der Deutschen Telekom, im Folgenden T-Com, entschieden haben.

Ihr Speedport 400P ist ein Breitband-Router (intelligentes Verbindungselement zwischen Netzen) mit integriertem DSL-Modem, der den Rechnern (Clients) in kabelgebundenen Inhausnetzen (LAN = Local Area Network) den Zugang zum Internet direkt über ADSL, z. B. T-DSL, ermöglicht. Er übernimmt im LAN (lokales Netz) den Verbindungsaufbau für alle Rechner zum öffentlichen Netz.

Die ISDN S0 Schnittstelle dient als Backup für die Internetverbindung und der Fernkonfiguration.

Dank des integrierten 4-Port Fast-Ethernet Switches können Sie bis zu vier kabelgebundene Rechner direkt anschließen. Wird Ihr kabelgebundenes Netzwerk größer, benötigen Sie zusätzliche Hubs/Switches.
Ihr Speedport 400P ermöglicht, dass mehrere Rechner im LAN über einen Anschluss auf das Internet zugreifen können.

Anschluss von einem oder mehreren Computern

Verfügt Ihr Rechners (Desktop oder Notebook) über eine Ethernet Buchse (LAN-Anschluss), so können Sie diesen Anschluss für die kabelgebundene Verbindung (Buchsen LAN1 - LAN4) zum Router verwenden. Es können bis zu vier LAN Geräte (Computer, IP Telefone, usw.) direkt an den Speedport 400P angeschlossen werden. Sollten weitere Geräte oder Computer angeschlossen werden, so können diese durch die Verwendung eines zusätzlichen Netzwerk-Switch angebunden werden.

Internetverbindung für alle Computer

Alle mit dem Speedport 400P verbundenen Computer können auf das Internet zugreifen. Die Internetverbindung wird von dem Speedport 400P aufgebaut. Dazu müssen im Speedport 400P die Internetzugangsdaten eingetragen sein.

Schutz durch integrierte Firewall

Jedes Netz kann durch technische Mittel abgehört werden.

Durch den Anschluss Ihres lokalen Netzes an das öffentliche Netz entstehen nicht unerhebliche Gefahren für die Sicherheit Ihrer Daten und Anwendungen. Grundsätzlich sollten Sie, wie beim Einzelanschluss, Ihre Rechner durch Virenscanner gegen heimtückische, versteckte Angriffe von außen, z. B. über die E-Mail, schützen.

Virenscanner schützen jedoch kaum gegen unberechtigten Zugriff von außen (Hacker).

Um dieser Gefahr entgegenzutreten, bietet Ihr Speedport 400P einen Schutz: durch die integrierte Firewall-Funktion. Wir empfehlen, dass Sie die Firewall zum Schutz gegen Angriffe einrichten und in Ihrem LAN die dort möglichen Schutzmaßnahmen aktivieren.

Gerät in Betrieb nehmen

Ihr Speedport 400P ist ein hochwertiges Gerät, das nur dann zu Ihrer Zufriedenheit arbeitet, wenn Sie alle für die Inbetriebnahme notwendigen Voraussetzungen beachten.

Gerät auspacken

Der Verpackungsinhalt besteht aus:

- VPN-Router Speedport 400P
- Steckernetzgerät (12 Volt DC, 1000 mA)
- Anschlussleitung zum T-DSL (Splitter) mit RJ45-Stecker (grau)
- Anschlussleitung zum ISDN mit RJ45-Stecker (grau)
- Ethernetkabel zum Anschluss von Netzwerkgeräten (gelb)
- RS-232 zu RJ-45 Konsolenstecker für die serielle Schnittstelle
- Mehrsprachige Installationsanleitung
- CD mit Software und deutschem Handbuch

Verpackungsinhalt überprüfen

Bevor Sie Ihren Speedport 400P in Betrieb nehmen, sollten Sie zunächst sorgfältig überprüfen, ob irgendwelche Schäden

- an der Verpackung darauf hindeuten, dass das Gerät beim Transport gestürzt ist!
- am Gehäuse oder
- am Steckernetzteil bzw. Netzkabel sichtbar sind! Auf keinen Fall dürfen Sie das Gerät in Betrieb nehmen, wenn es beschädigt ist! Wenden Sie sich im Zweifelsfall an den Technischen Kundendienst unter der Rufnummer

0180 5 443030. Der Verbindungspreis beträgt 0,12 € pro angefangene 60 Sekunden bei einem Anruf aus dem T-Com Festnetz (Stand August 2005).

Tipp

Heben Sie die Originalverpackung des Gerätes auf. Sie können sie dann für einen Transport anlässlich eines Umzuges oder zum Versand des Gerätes verwenden.

Aufstellungsort

Der Aufstellort des Speedport 400P muss sich in der Nähe einer Stromsteckdose befinden.
Die Verbindung des Speedport 400P zum Splitter findet über Ethernetkabel statt. Das im Lieferumfang dafür enthaltene Kabel hat eine Länge von ca. 3 m. Ist die Entfernung zum Splitter größer, können Sie ein längeres Ethernetkabel erwerben und einsetzen.

Aufstellen des Speedport 400P

Ihr Speedport 400P ist für den Tischbetrieb vorgesehen.

!

Die heutigen Möbel sind mit einer unübersehbaren Vielfalt von Lacken und Kunststoffen beschichtet und werden mit unterschiedlichen Lackpflegemitteln behandelt. Es ist nicht auszuschließen, dass manche dieser Stoffe Bestandteile enthalten, welche die Kunststofffüße angreifen und erweichen. Die so durch Fremdstoffe veränderten Gerätefüße können auf der Oberfläche der Möbel unliebsame Spuren hinterlassen. Die Deutsche Telekom AG, T-Com kann aus verständlichen Gründen für derartige Schäden nicht haften.

Wandmontage

Sie können Ihren Speedport 400P auch an der Wand befestigen. Dafür sind auf der Unterseite Bohrungen angebracht. Achten Sie beim Befestigen darauf, dass die LEDs sichtbar bleiben und die Kabel nicht geknickt werden. Schrauben und Dübel sind nicht im Lieferumfang enthalten. Eine Bohrschablone ist beigelegt.

!

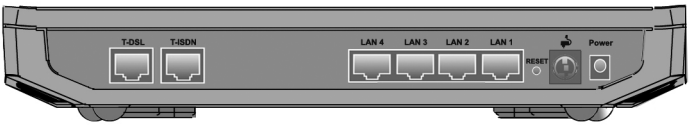
Beachten Sie beim Anbringen der Schrauben alle handwerklichen Vorsichtsmaßnahmen, z. B. beim Bohren und Dübeln. Aus verständlichen Gründen kann T-Com nicht für dadurch entstehende Schäden haften.

Anschließen

Ihr Speedport 400P darf noch nicht an das Stromnetz angeschlossen sein und der Rechner, den
Sie über das Ethernetkabel mit dem Gerät verbinden, sollte ausgeschaltet sein.

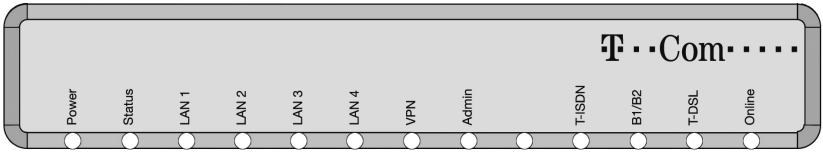
Anschlüsse auf der Rückseite des Speedport 400P

Port	Bedeutung
On / Off	EIN / AUS Schalter
DC12V/1A	Schließen Sie das mitgelieferte Netzteil an.
RESET	Durch Drücken des Resettaste kann ein Neustart des Gerät durchgeführt werden oder es werden die Werkseinstellungen wiederhergestellt. Durch Drücken des Resettaste wird bei: 0 - 3 Sekunden - ein Neustart des Gerätes erfolgen über 6 Sekunden – eine Wiederherstellung der Werkseinstellungen (dies wird verwendet wenn Sie sich nicht mehr einloggen können oder das Passwort vergessen haben).
LAN 1X — 4X (RJ-45 Anschluss)	Schließen Sie ein UTP Ethernet Kabel an einen dieser 4 Ports, wenn Sie eine Verbindung zu einem 10 MBit/s oder 100 MBit/s LAN aufbauen möchten. Der LAN Port 4 dient auch als Anschluss für das Konsolenkabel.
T-DSL	Schließen Sie hier das mitgelieferte RJ45-RJ45-Kabel an und verbinden es mit dem Splitter.
ISDN	Schließen Sie hier das mitgelieferte RJ45-RJ45-Kabel an und verbinden es mit dem NTBA, wenn Sie das ISDN Backup oder die Fernkonfiguration verwenden wollen.



Anzeigen

Ihr Speedport 400P ist mit Leuchtanzeigen (LEDs) ausgestattet, welche folgende Bedeutung haben.

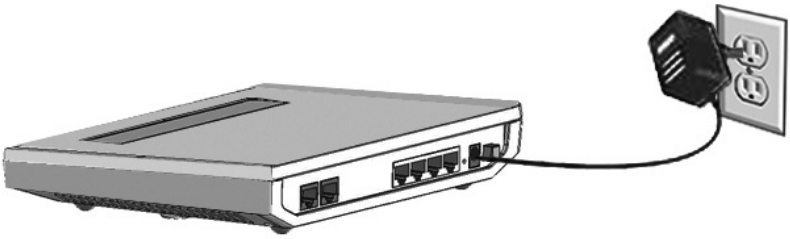


Bezeichnung	Farbe	Zustand	Funktion
Power		Aus	Gerät ohne Strom
	Grün	An	Gerät ist eingeschaltet
Status		Aus	Gerät ist ausgeschaltet
	Grün	An	Gerät ist Betriebsbereit
		Blinkt	Gerät startet
LAN 1		Aus	Keine aktive Netzwerkverbindung
LAN 2	Grün		
		An	LAN Verbindung mit 100 MBit/s hergestellt
LAN 3		Blinkt	Daten werden gesendet/empfangen
LAN 4	Orange		
		An	LAN Verbindung mit 10 MBit/s hergestellt
		Blinkt	Daten werden gesendet/empfangen
VPN	Grün	Aus	Keine VPN Verbindung
		An	VPN Tunnel hergestellt
Admin	Grün	Aus	Fernkonfiguration deaktiviert
		An	Fernkonfiguration aktiviert
T-ISDN		Aus	Keine ISDN Verbindung
	Grün	An	Leuchtet bei einer ISDN Verbindung und/oder wenn der S0 Bus aktiv ist.
B1/B2		Aus	Keine ISDN Verbindung
	Grün	An	Zeigt eine erfolgreiche Verbindung über den ISDN B1 Kanal an.
	Orange	An	Zeigt eine erfolgreiche Verbindung über den ISDN B2 Kanal an
T-DSL		Aus	Gerät ist aus oder die Synchronisation ist noch nicht gestartet
	Grün	An	Erfolgreiche Synchronisation mit dem DSLAM
		Blinkt	Synchronisation mit DSLAM wird durchgeführt
Online		Aus	Keine Internetverbindung
	Grün	An	Internetverbindung hergestellt

Speedport 400P an die Stromversorgung anschließen

Nur das beiliegende Netzteil für den Speeport 400P verwenden.

Stecken Sie den Stecker des dünnen Kabels in die Anschlussbuchse für das Steckernetzgerät im Speedport 400P. Schließen Sie das Steckernetzgerät über eine eigene 230 V Steckdose an. Schalten Sie Ihren Router ein, sodass die Anzeige Power leuchtet.

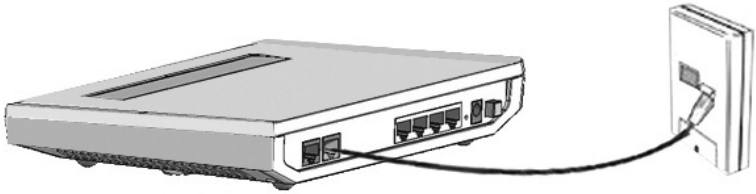


Stecken Sie das Netzteil nie in eine Stromsteckdose, von der Sie nicht sicher sind, dass sie den auf dem Typenschild angegebenen Werten entspricht: Netzteil und Gerät können zerstört werden, Sie können körperlichen Schaden erleiden.

Sollten Sie eine Verlängerungsschnur mit Steckerleiste verwenden, achten Sie darauf, dass die Leistungsaufnahme aller an der Leiste angeschlossenen Geräte nicht die zugelassene Belastung des Kabels übersteigt. Brandgefahr!

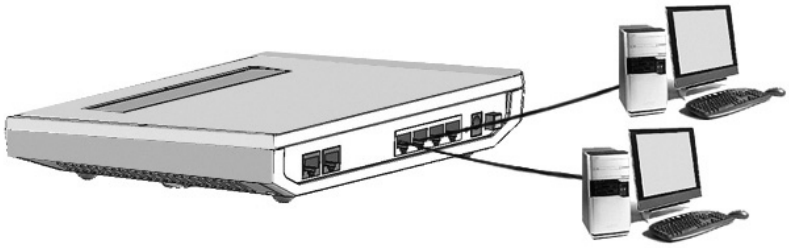
Speedport 400P am DSL anschließen

Stecken Sie eines der im Lieferumfang enthaltenen RJ-45 Kabel in die T-DSL-Buchse am Speedport 400P. Das andere Ende stecken Sie in die mit „DSL“ beschriftete Buchse den Splitters. Nach erfolgreichem Aufbau der DSL-Verbindung leuchtet die LED T-DSL.



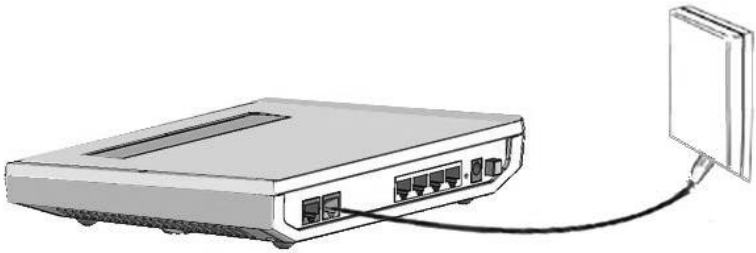
Speedport 400P mit dem LAN Anschluss des Computers verbinden

Für den Anschluss an das lokale, kabelgebundene Netz (LAN) stecken eines der beiliegenden Ethernetkabel in die mit LAN gekennzeichnete Buchsen an der Rückseite des Gerätes (die Ports sind gelb markiert). Das andere Ende stecken Sie in die Buchse der Ethernet-Schnittstellenkarte an Ihrem Rechner.



ISDN-Anschluss (optional)

Stecken Sie eines der im Lieferumfang enthaltenen RJ-45 Kabel in die ISDN-Buchse am Speedport 400P. Das andere Ende stecken Sie in den NTBA. Nach erfolgreichem Aufbau der ISDN-Verbindung leuchtet die LED ISDN.



Konfiguration des Speedport 400P

Nachdem Sie den Speedport 400P angeschlossen und mit einem Computer verbunden haben, können sie den Speedport 400P konfigurieren. Für die Konfiguration wird ein Standard Web Browser verwendet, welcher mit Ihrem Betriebssystem schon mitgeliefert wird, daher benötigen Sie keine spezielle Installationssoftware. Die Konfiguration ist sehr einfach und benutzerfreundlich.

Vorbereiten des einzubindenden Rechners/Netzwerkes

!

Das im Folgenden beschriebene Prüfen der Netzwerkkarte und der Eigenschaften von TCP/IP ist für Rechner nur in den Fällen notwendig, in denen diese Rechner nach dem Einbinden im Netz nicht erreichbar sind. Es ist Ihnen freigestellt, ob Sie diese Prüfung noch vor dem eigentlichen Einrichten des Routers vornehmen oder ob Sie die Prüfung zunächst überspringen. Sollte für die Ethernetkarte kein TCP/IP Protokoll installiert sein, kann keine Verbindung zum Router aufgebaut werden. Kehren Sie dann zu diesem Kapitel zurück und führen Sie die Prüfung und Einstellung der Ethernetkarte durch.

Tipp

Läuft der ins Netzwerk einzubindende Rechner unter Windows® XP oder Windows 2000, ist im Regelfall das Einrichten der Netzwerkkarte nicht notwendig, da XP bereits DHCP-orientiert ist und als Standard TCP/IP als Transportprotokoll verwendet.

Prüfen der Netzanbindung der Ethernetkarte

Dieser Vorgang wird am Beispiel der Betriebssysteme Windows® XP und 2000 gezeigt. Windows® XP ist bereits von vornherein auf das Unterstützen eines DHCP-Servers ausgelegt und bindet im Regelfall Netzwerkkarten über TCP/IP in lokale Netze ein.

Die Anbindung mit den Betriebssystemen Windows® NT, 95, 98, ME (Millenium Edition) wird in der Bedienungsanleitung auf der beiliegenden CD beschrieben.

Tipp

Ist die Ethernetkarte nicht an TCP/IP gebunden, müssen Sie die Bindung vornehmen. War beim Installieren des Betriebssystems das Übernehmen der Netzwerkprotokolle nicht vorgesehen, werden Sie im Verlauf des Vorgangs aufgefordert, Ihre CD-ROM mit dem Betriebssystem einzulegen.

Konfiguration des PCs unter Windows XP

1. Gehen Sie zu Start / Einstellungen / Systemsteuerung (bei klassischer Ansicht). In der Systemsteuerung, doppelklick auf Netzwerkverbindungen.

2. Doppelklicken auf LAN-Verbindung. (Siehe Bild 3.1)

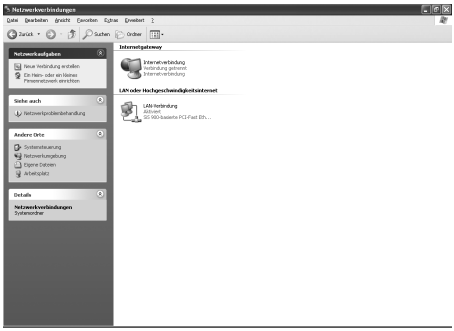


Bild 3.1: LAN Verbindung

3. Im Fenster Status von LAN-Verbindung klicken Sie auf Eigenschaften. (Siehe Bild 3.2)

Bild 3.2: Status von LAN Verbindung

4. Wählen Sie Internet Protokoll (TCP/IP) und klicken Sie auf Eigenschaften. (Siehe Bild 3.3)

Bild 3.3: TCP / IP

5. Wählen Sie IP-Adresse automatisch beziehen und dann darunter DNS-Serveradresse automatisch beziehen. (Siehe Bild 3.4)

6. Klicken Sie auf OK um die Konfiguration zu beenden.

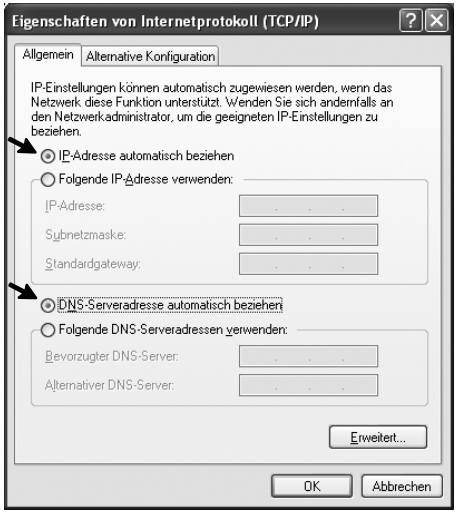


Bild 3.4: IP Adresse & DNS Konfiguration

Konfiguration des PCs unter Windows 2000

1. Gehen Sie auf Start / Einstellungen / Systemsteuerung. Doppelklicken Sie dort auf Netzwerk und DFÜ-Verbindungen.

2. Doppelklicken Sie auf LAN-Verbindung. (Siehe Bild 3.5)

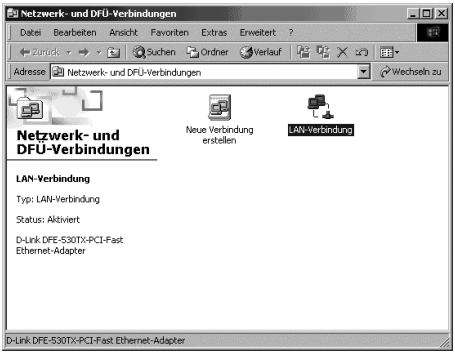


Bild 3.5: LAN Verbindung

3. Im Fenster Status von LAN-Verbindung klicken Sie auf Eigenschaften. (Siehe Bild 3.6)

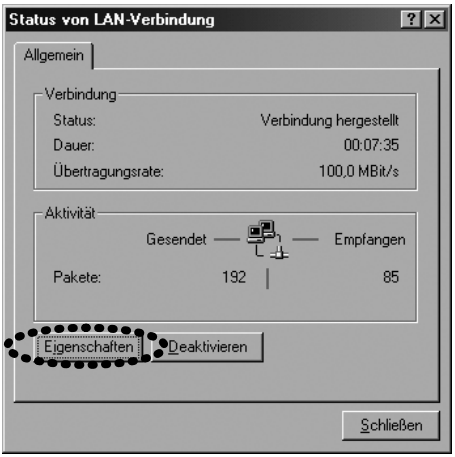


Bild 3.6: LAN Verbindung

4. Wählen Sie Internetprotokoll (TCP/IP) und klicken dann auf Eigenschaften. (Siehe Bild 3.7)

Bild 3.7: TCP / IP

5. Wählen Sie IP-Adresse automatisch beziehen und dann darunter DNS-Serveradresse automatisch beziehen. (Siehe Bild 3.8)

6. Klicken Sie auf OK um die Konfiguration zu beenden.

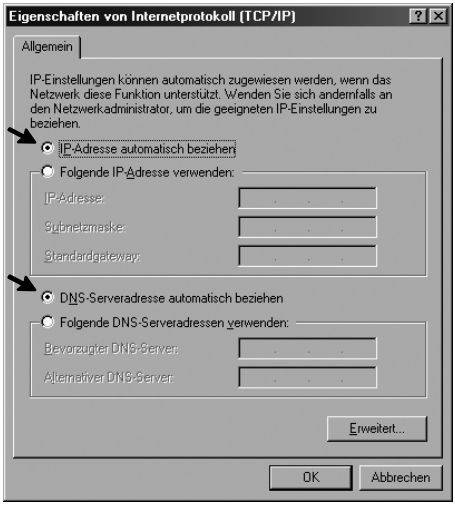


Bild 3.8: IP Adresse & DNS Konfiguration

Erstkonfiguration

Ihr Speedport 400P ist bereits so vorkonfiguriert, dass er im Regelfall ohne umfangreiche Feinkonfiguration lauffähig ist. Daher empfehlen wir, die Erstinstallation mit Hilfe des Einrichtungsassistenten vorzunehmen. Der Einrichtungsassistenten ist in den Web-Konfigurator integriert und führt Sie durch wenige Bereiche, die für den Betrieb unabdingbar sind. Sie können danach jederzeit eine Feinkonfiguration durchführen.

Tipp

Bevor Sie mit dem Konfigurieren beginnen, legen Sie bitte die Unterlagen (Auftragsbestätigung), die Sie nach Ihrer Anmeldung bei einem Dienstanbieter, z. B. T-Online International, erhalten haben, griffbereit. Sie benötigen die Angaben mit den persönlichen Daten, damit Sie eine Verbindung zum Dienstanbieter (Provider) ins Internet aufbauen können.

Der Web-Konfigurator

Der Web-Konfigurator basiert auf HTML. Sie rufen das Konfigurationsprogramm mit einem Internet-Browser auf. Sie können dafür den Browser verwenden, der auf Ihrem Rechner installiert ist (z. B. Internet Explorer ab 5.5 oder Netscape ab 7.0 oder ein Browser, der Java-Script unterstützt und bei dem Pop-Up Fenster nicht blockiert sind) und den Sie für sich als Ihren Standard-Browser verwenden möchten. Das Vorgehen ist in allen Fällen das gleiche. Im Beispiel ist der Internet Explorer®der Microsoft Corporation dargestellt. Sie können ebenso den Netscape Navigator®, Opera®oder andere verwenden.

Öffnen Sie Ihren Internet-Browser. Rufen Sie den Web-Konfigurator auf, indem Sie die IP-Adresse Ihres Speedport 400P eingeben. Diese lautet bei Auslieferung: 192.168.2.1. Bestätigen Sie Ihre Eingabe mit Enter.

Tipp

Die Einstellungen Ihres Browsers muss das Anzeigen von Pop-Ups akzeptieren, Java Script muss aktiviert sein, es darf kein automatisches Konfigurationsskript verwendet werden und es darf kein Proxyserver (Proxy = Stellvertreter; Bindeglied/Puffer im Netz zwischen dem Rechner und dem Netzserver) definiert sein.

Konfiguration mit dem Einrichtungsassistent

Sie haben, wie beschrieben, Ihren Speedport 400P angeschlossen und gegebenenfalls die Protokollanbindung der Ethernetkarte und die Eigenschaften von TCP/IP überprüft. Ihr Router ist an das Stromnetz angeschlossen und mittels der Ethernetkabel die physische Verbindung des Routers zum Splitter und dem Rechner, von dem aus Sie konfigurieren möchten, hergestellt.

Schalten Sie den Router über den Netzschalter ein. Warten Sie bis die Kontroll-LED für Power (Betrieb) und System, DSL (gegebenenfalls ISDN) und LAN leuchten.

Klicken Sie auf das Symbol des von Ihnen verwendeten Internet-Browsers, z. B.

für den Internet Explorer ab 5.5

oder

für den Netscape Navigator ab 7.0

oder jeden anderen Internet-Browser, sofern er die Voraussetzungen wie im Tipp auf der vorherigen Seite beschrieben, erfüllt. Sie können die Anwendung auch aufrufen über Start -> Programme, sich aus der Liste den Browser aussuchen und darauf klicken.

Tipp

Im Folgenden geben Sie die Adresse für das Konfigurationsprogramm ein. Beachten Sie dabei bitte:
Geben Sie als URL nur die IP-Adresse 192.168.2.1 ein. Sie können auch http:// und dann die IP-Adresse eingeben, aber nie www. Das Konfigurationsprogramm wird in diesem Fall nicht gefunden, es erscheint Seite nicht verfügbar.

Das Fenster des von Ihnen gewählten Browsers wird geöffnet.

Wahrscheinlich wird der Browser versuchen eine Verbindung ins Internet aufzubauen. Brechen Sie diesen Vorgang durch Drücken der Taste ESC auf der Tastatur Ihres Rechners ab. Das Hinweisfenster Aktion abgebrochen erscheint.

Geben Sie in der Adressleiste die URL des Konfigurationsprogramms ein:
192.168.2.1

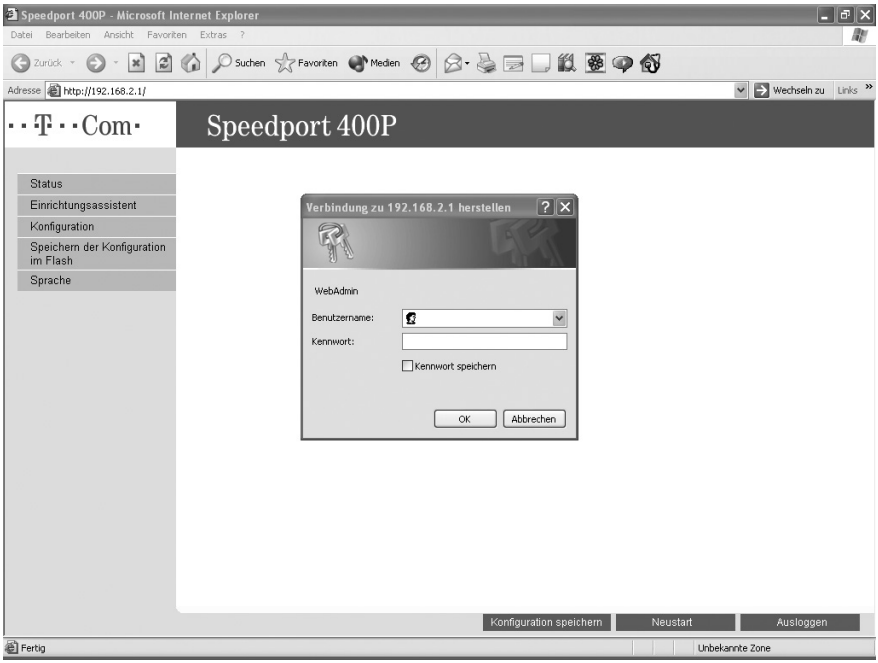
Drücken Sie die Zeilenschalttaste (Return, Enter).

Klicken Sie auf OK.

Das Fenster zum Einloggen wird angezeigt.

Tipp

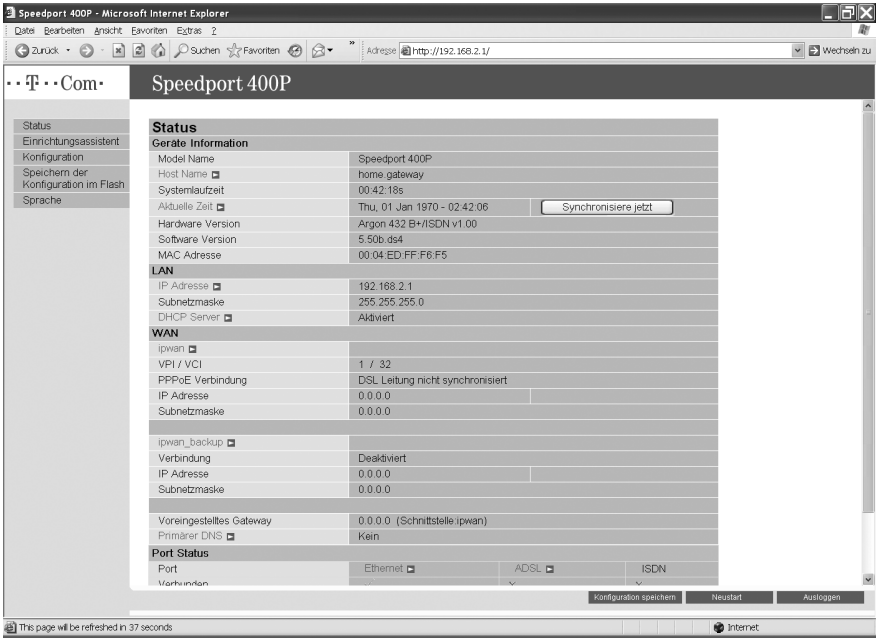
Wird das Fenster nach kurzer Zeit nicht geöffnet, und erscheint stattdessen das Fenster „Seite nicht verfügbar“, haben Sie die URL falsch eingegeben oder die Gateway Adresse auf Ihrem Rechner wurde nicht oder falsch vergeben. Prüfen Sie die Eigenschaften von TCPI/IP (siehe Seite 11 folgend). Führt auch das nicht zum Erfolg, siehe Problembehandlung (Seite 174 folgend).



Geben Sie als Benutzernamen **admin** ein. Geben Sie als Kennwort ebenfalls **admin** ein. Die Eingabe wird als Punkte oder Sternchen dargestellt.

Hatten Sie den Router bereits konfiguriert und möchten Sie jetzt Änderungen oder Erweiterungen
vornehmen, geben Sie an dieser Stelle den Benutzernamen und das Kennwort ein, das Sie selbst vergeben haben.

Nach kurzer Zeit sehen Sie die Statusseite des Speedport 400P (Die Beschreibung der Statusseite finden Sie im Kapitel Erweiterte Konfiguration).



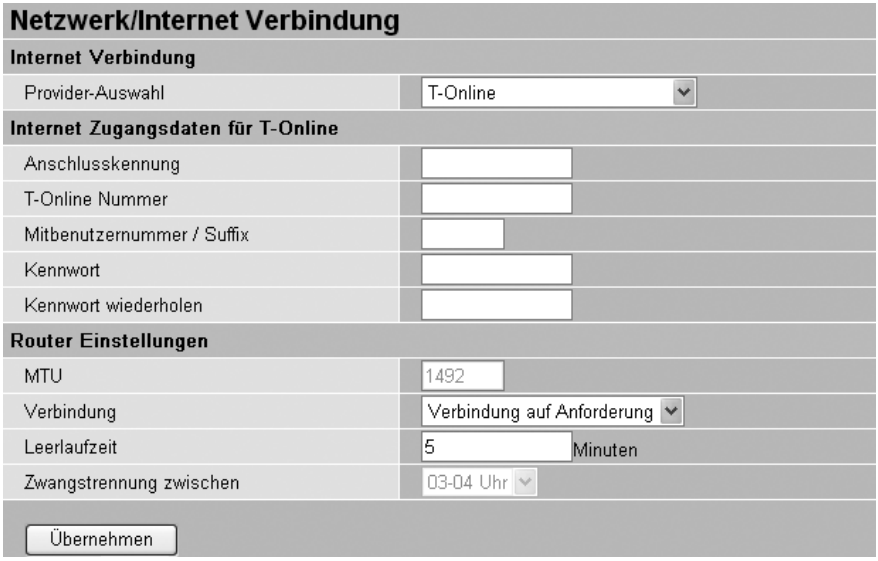
Sie haben die Wahl den Einrichtungsassistenten zu wählen (im Folgenden verwendet) oder über Konfiguration erweiterte Einstellungen vorzunehmen.

Einrichtungsassistent

Der Einrichtungsassistent hilft Ihnen mit wenigen Schritten die Internetverbindung über ADSL zu erstellen.
Klicken Sie im Menü links auf Einrichtungsassistent.

Tipp

T-Online ist voreingestellt und in diesem Abschnitt beschrieben, klicken Sie auf den Aufklapp-Pfeil im Menü Provider-Auswahl für die weiteren Dienstanbieter T-DSL Business mit dyn. IP, T-DSL Business mit fester IP, Anderer Anbieter. Die vorgehensweise der Einrichtung der weiteren Dienstanbieter wird im Kapitel Einrichtungassistent beschrieben.



Die hier geforderten Daten wie Anschlusskennung, T-Online Nummer, Mitbenutzersuffix und Kennwort wurden Ihnen von Ihrem Dienstanbieter in einem Geheimumschlag vorgegeben. Bewahren Sie diese Daten unzugänglich für Unbefugte auf, denn mit diesen Angaben könnten Fremde auf Ihren Namen und auf Ihre Kosten im Internet surfen.

Geben Sie die erforderlichen Daten ein. Beachten Sie dass Sie das Kennwort zweimal eintragen müssen. Die Eingabe des Kennwort und Kennwort wiederholen wird als Punkte oder Sternchen dargestellt.

Die Angaben unter Router Einstellungen dienen dem Einstellen der Art des Internetzugriffs. Was Sie hier einstellen ist im Besonderen auch davon abhängig, welchen Tarif Sie beauftragt haben.

- Die Grundeinstellung lautet Verbindung auf Anforderung mit einer Leerlaufzeit von 5 Minuten. Die Verbindung zum Internet wird nur aufgebaut wenn Sie z.B. den Browser öffnen oder Emails abrufen. Messenger Programme oder Programme welche ein automatisches Update durchführen veranlassen den Router ebenfalls die Verbindung zum Internet aufzubauen. Nach 5 Minuten ohne Datentransfer wird die Verbindung beendet.

- Aktivieren Sie die Option Ständig verbunden baut der Speedport 400P die Verbindung nicht ab, sondern bleibt immer mit dem Internet verbunden. Zusätzlich können Sie bestimmen wann die Zwangstrennung erfolgen soll.

Wir empfehlen die Option Ständig verbunden nur dann zu aktivieren, wenn Sie über eine Flatrate verfügen. Ansonsten können sehr hohe Kosten anfallen.

Nachdem Sie alle Angaben eingetragen haben, klicken Sie auf Übernehmen.

Klicken Sie auf Konfiguration speichern und bestätigen Sie das Speichern der Konfiguration indem Sie auf Übernehmen klicken.

Wird die Konfiguration nicht gespeichert, werden die Einstellungen bei einem Neustart oder Stromausfall verworfen.

Ausloggen

Um das Web Interface des Routers zu verlassen, wählen Sie **Ausloggen.** Vergewissern Sie sich, daß Sie die Konfiguration gespeichert haben, bevor Sie ausloggen.

Bedenken Sie, daß der Router sich nur von einem PC gleichzeitig konfigurieren läßt. Sobald ein PC auf den Router zugreift, kann kein anderer einen Zugriff darauf erhalten, solange der PC sich nicht ausgeloggt hat. Wenn der vorherige PC sich vergisst auszuloggen, so kann der zweite PC nach einer vorgegeben Zeit — der Standardwert ist 3 Minuten — auf den Router zugreifen.

Im Internet surfen

Klicken Sie auf Status. Im Statusfenster unter WAN (Wide Area Network) wird der Status der Internetverbindung (PPPoE Verbindung) angezeigt. Wird Verbindung auf Anforderung aktiviert angezeigt, klicken Sie auf das Symbol Ihres Internet-Browsers. Der Browser wird geöffnet und die für den Browser eingestellte Startseite wird im Internet gesucht und geöffnet. Wird Verbindung hergestellt angezeigt können Sie ebenfalls im Internet surfen. Zusätzlich sehen Sie die aktuelle Verbindungszeit, sowie die Zeit bis zum Auflegen der Verbindung. Die Statusseite wird alle 60 Sekunden aktualisiert.

Möchten Sie eine andere Seite besuchen, z. B. die von T-Online, doppelklicken Sie in die Adresszeile des Browsers, und geben Sie www.t-online.de ein. Drücken Sie anschließend die Enter-Taste. Die Startseite von T-Online wird aufgerufen.

Tipp

Wird das Fenster des erfolgreichen Verbindungsaufbaus nicht in einer Form, die der abgebildeten ähnlich ist, angezeigt, sondern mit einem Fehlerhinweis, konnte keine Verbindung ins Internet hergestellt werden.

Das kann daher rühren, dass

- Sie bei dem angegebenen Dienstanbieter noch nicht angemeldet sind. Rufen Sie die Hotline an und fragen Sie nach.
- Ihnen bei der Eingabe der Daten des Dienstanbieters Fehler unterlaufen sind. Wiederholen Sie die Konfiguration über den Assistenten.
- Die Kabelverbindung zwischen Router und Splitter nicht richtig ist. Prüfen Sie die Verbindungskabel.

Erweiterte Konfiguration

Dieses Kapitel beschreibt die erweiterten Konfigurationseinstellungen des Speedport 400P. Im Regelfall sind Änderungen dieser Einstellungen für den Betrieb des Speedport 400P nicht notwendig.

Diese Einstellungen sollten Sie nur vornehmen, wenn Sie sich sicher sind, was diese Einstellungen bewirken.

Wird die Konfiguration nicht gespeichert, werden die Einstellungen bei einem Neustart oder Stromausfall verworfen.

Auf der Konfigurations-Webseite befindet sich auf der linken Seite ein Navigations-Menü. Dort finden Sie Links, die Sie direkt zu den gewünschten Einstellungen führen. Inklusive:

Status

(ARP Tabelle, Routing Tabelle, DHCP Tabelle, PPTP Status, IPSec Status, L2TP Status, Email Status, Ereignis Protokoll, Fehler Protokoll, NAT Sitzungen, Diagnose und UPnP Portmap)

Einrichtungsassistent

Konfiguration

(LAN, WAN, System, Firewall, VPN, QoS, Virtual Server, Zeitplan und Erweitert)

Speichern der Konfiguration im Flash

Sprache

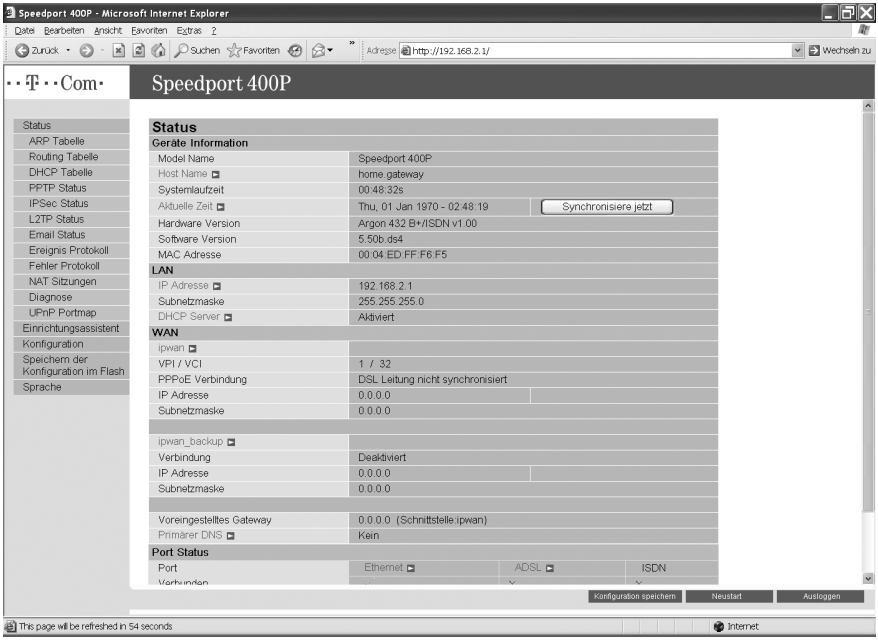
(Der Web-Konfigurator unterstützt die Sprachen Deutsch und Englisch)

Status

Wenn Sie dieses Feld anklicken, erhalten Sie die Statusseite und folgendes Untermenü.

(ARP Tabelle, Routing Tabelle, DHCP Tabelle, PPTP Status, IPSec Status, L2TP Status, Email Status, Ereignis Protokoll, Fehler Protokoll, NAT Sitzungen, Diagnose und UPnP Portmap)

Statusseite



Die Statusseite zeigt Ihnen den aktuellen Zustand des Routers.

Geräte Information

Model Name:

Die Bezeichnung Ihres Routers.

Host Name:

Der Host Name Ihres Routers. Wenn Sie den Host Namen in der Adresszeile Ihres Browser eingeben gelangen Sie ebenfalls zum Web-Konfigurator.

Systemlaufzeit:

Die Systemlaufzeit des Routers seit dem letzten Neustart.

Aktuelle Zeit:

Die aktuelle Zeit. In der Werkseinstellung wird diese nach einer erfolgreichen Internetverbindung mit einem SNTP Server abgeglichen. Weitere Informationen finden Sie im Kapitel Zeitzone.

Hardware Version:

Die verwendete Hardware Ihres Routers. Bitte halten Sie diese Information bereit sofern Sie sich bei technischen Problemen mit der Service-Hotline in Verbindung setzen. Weitere Informationen zum Support finden Sie im Kapitel Anhang.

Software Version:

Die verwendete Software Ihres Routers, auch Firmware genannt. Bitte halten Sie diese Information bereit sofern Sie sich bei technischen Problemen mit der Service-Hotline in Verbindung setzen. Weitere Informationen zum Support finden Sie im Kapitel Anhang.

MAC Adresse:

Die MAC Adresse des Routers.

LAN

IP Adresse:

Die IP Adresse des Routers. Werksseitig ist die IP Adresse 192.168.2.1 voreingestellt.

Subnetz Maske:

Die Subnetz Maske des Routers. Werksseitig ist die Subnetz Maske 255.255.255.0 voreingestellt.

DHCP Server:

Der Status des DHCP Servers.

WAN

IPWAN (Internet Verbindung über DSL)

VPI/VCI:

Die verwendeten VPI/VCI Werte. In der Regel wird in Deutschland 1/32 verwendet.

PPPoE Verbindung:

Status der PPPoE Verbindung. Wenn eine PPPoE Verbindung besteht kann diese durch den Button „Verbindung trennen“ getrennt werden. Je nachdem ob Sie Verbindung auf Anforderung oder Ständig verbunden ausgewählt haben wird die Verbindung zum Internet Provider wieder hergestellt.

IP Adresse:

Vom Internet Provider zugewiesene, öffentliche IP Adresse des Routers.

Subnetzmaske:

Vom Internet Provider zugewiesene, öffentliche Subnetz Maske des Routers.

WAN

IPWAN Backup (Internet Verbindung über ISDN, optional)

Verbindung:

Status der Backup ISP Verbindung über ISDN.

IP Adresse:

Vom Internet Provider zugewiesene, öffentliche IP Adresse des Routers.

Subnetzmaske:

Vom Internet Provider zugewiesene, öffentliche Subnetz Maske des Routers.

Voreingestelltes Gateway:

Die Gateway Adresse für die Internetverbindung des Routers.

Primärer DNS:
Die primäre DNS Adresse für die Internetverbindung.

Ports Status

Port:
Listed die verschiedenen Ports auf.

Verbunden:
Zeigt den Status der Ports grafisch an.

Statistiken:
Informationen über Einstellungen und gesendeten/empfangenen Paketen.

ARP Tabelle

Information der ARP (Address Resolution Protocol) Tabelle, welche zu den entsprechenden Internet (IP) Adressen die zugehörige Ethernet (MAC) Adresse anzeigt. Diese ist sehr nützlich um die MAC Adressen der angeschlossenen PCs für die Funktionen Firewall – MAC Adressen Filter zu nutzen. Weitere Informationen finden Sie im Abschnitt Firewall in dieser Anleitung.

ARP Tabelle

IP <> MAC Liste

IP Adresse	MAC Adresse	Schnittstelle	Statisch
192.168.2.101	00:0b:6a:ae:c7:a1	iplan	no

IP Adresse: Eine Liste von IP Adressen Ihrer Geräte im LAN (Local Area Network).

MAC Adresse: Die MAC (Media Access Control) Adresse für jedes Gerät in Ihrem LAN.

Schnittstelle: Der Name der Schnittstelle (am Router) wo diese IP verbunden ist.

Statisch: Status des ARP Tabelleneintrages:

- **"no"** für dynamisch-generierte ARP Tabelleneinträge
- **"yes"** für statische ARP Tabelleneinträge die vom Benutzer hinzugefügt worden sind

Routing Tabelle

Routing Tabelle

Routing Tabelle

Gültig	Ziel	Netzmaske	Gateway/Schnittstelle	Kosten
✓	0.0.0.0	0.0.0.0	0.0.0.0/ ipwan	1

RIP Routing Tabelle

Ziel	Netzmaske	Gateway	Kosten

Routing Tabelle

Gültig:
Zeigt einen erfolgreichen Routing Status an.

Ziel:
Die IP Adresse des Ziel Netzwerk.

Netzmaske:
Die Ziel Netzmaske Adresse.

Gateway/Schnittstelle:
Die IP Adresse des Gateway oder Schnittstelle die diese Route benutzt.

Kosten:
Die Anzahl der Hops zählt als Kosten der Route.

RIP Routing Tabelle

Ziel:
Die IP Adresse des Ziel Netzwerk.

Netzmaske:
Die Ziel Netzmaske Adresse.

Gateway:
Die IP Adresse des Gateway welches diese Route benutzt.

Kosten:
Die Anzahl der Hops zählt als Kosten der Route.

DHCP Tabelle

Leased:
Die DHCP zugeordneten IP Adressen Information.

Abgelaufen:
Die abgelaufenen IP Adress- Informationen

Permanent:
Die Fixed Host mapping Informationen.

Leased Tabelle

Leased Tabelle			
IP Adresse	MAC Adresse	Client Host Name	Fristablauf
192.168.2.101	00:0b:6a:ae:c7:a1	test	11 hours

IP Adresse:
Die IP Adresse die diesem Client zugeordnet ist.

MAC Adresse:
Die MAC Adresse des Clients.

Client Host Name:
Der Host Name (Computer Name) des Client.

Fristablauf:
Die aktuelle Ablaufzeit des Clients.

Fristablauf Tabelle

Fristablauf Tabelle			
IP Adresse	MAC Adresse	Client Host Name	Fristablauf
192.168.2.100	00:0b:6a:ae:c7:a1	test	Expired

Bitte schauen Sie bei der Leased Tabelle nach.

Permanent Tabelle

Permanent Tabelle			
Name	IP Adresse	MAC Adresse	Maximale Lease Zeit

Name:
Der Name den Sie der permanenten Konfiguration zugeordnet haben

IP Adresse:
Die feste IP Adresse des speziellen Clients.

MAC Adresse:

Die MAC Adresse die Sie der festen IP Adresse zuordnen wollen.

Maximale Lease Zeit:

Das maximale Lease Zeit Intervall welches Sie den Clients erlauben.

PPTP Status

Details Ihrer PPTP VPN Konfiguration und Status der Verbindung.

PPTP Status

VPN/PPTP für Remote Access Anwendungen

Name	Typ	Aktivieren	Aktiv	Tunnel Verbunden	Anruf Verbunden	Verschlüsselung

VPN/PPTP für LAN-to-LAN Anwendungen

Name	Typ	Aktivieren	Aktiv	Tunnel Verbunden	Anruf Verbunden	Verschlüsselung

Name:

Name der PPTP Verbindung welchen Sie in der VPN Konfiguration angegeben haben.

Typ:

Typ der Verbindung (Ein-/Ausgehend).

Aktivieren:

Zeigt an ob die Verbindung aktiviert ist.

Aktiv:

Zeigt an ob aktuell eine Verbindung aktiv ist.

Tunnel Verbunden:

Zeigt an ob der VPN Tunnel verbunden ist.

Anruf Verbunden:

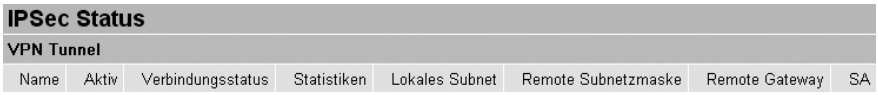
Zeigt an ob der Anruf für diesen VPN Eintrag aktuell verbunden ist.

Verschlüsselung:

Zeigt die Art der Verschlüsselung für diese VPN Verbindung an.

IPSec Status

Details Ihrer IPSec VPN Konfiguration und Status der Verbindung.



Name:

Name der IPSec Verbindung welchen Sie in der VPN Konfiguration angegeben haben.

Aktiv:

Zeigt an ob die VPN Verbindung aktiv ist.

Verbindungsstatus:

Zeigt an ob die VPN Verbindung verbunden oder getrennt ist.

Statistiken:

Statistiken für diese VPN Verbindung.

Lokales Subnet:

Die lokale IP-Adresse oder Subnetz welches verwendet wird.

Remote Subnetzmaske:

Die Subnetzmaske des entfernten Netzes.

Remote Gateway:

Die IP-Adresse des entfernten Gateways.

SA:

Zeigt die Security Association für den VPN Eintrag.

L2TP Status

Details Ihrer L2TP VPN Konfiguration und Status der Verbindung.

L2TP Status

VPN/L2TP für Remote Access Anwendung

Name	Typ	Aktivieren	Aktiv	Tunnel Verbunden	Anruf Verbunden	Verschlüsselung

VPN/L2TP für LAN-to-LAN Anwendung

Name	Typ	Aktivieren	Aktiv	Tunnel Verbunden	Anruf Verbunden	Verschlüsselung

Name:
Name der L2TP Verbindung welchen Sie in der VPN Konfiguration angegeben haben.

Typ:
Typ der Verbindung (Ein-/Ausgehend).

Aktivieren:
Zeigt an ob die Verbindung aktiviert ist.

Aktiv:
Zeigt an ob aktuell eine Verbindung aktiv ist.

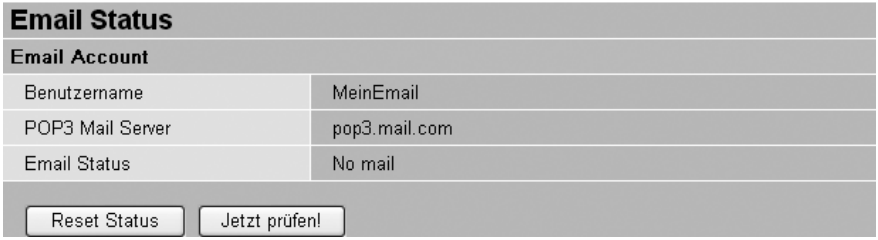
Tunnel Verbunden:
Zeigt an ob der VPN Tunnel verbunden ist.

Anruf Verbunden:
Zeigt an ob der Anruf für diesen VPN Eintrag aktuell verbunden ist.

Verschlüsselung:
Zeigt die Art der Verschlüsselung für diese VPN Verbindung an.

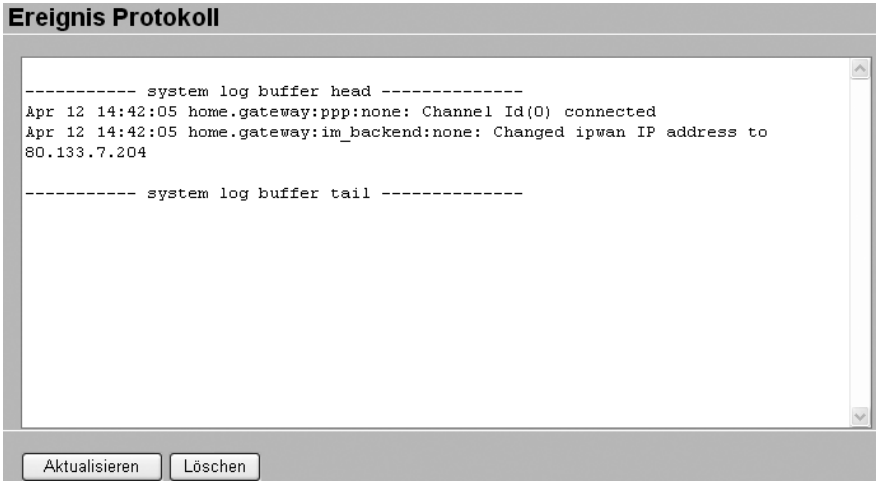
Email Status

Details und Status für Ihren Email Account welchen Sie für die Überprüfung konfiguriert haben. Lesen Sie weitere Informationen darüber im Abschnitt Erweitert in dieser Anleitung.



Ereignis Protokoll

Diese Seite zeigt die Router Ereignisanzeige an. Wichtige System-Protokollierungs-Informationen sind dort vorhanden, wie ADSL Verbindung abgebrochen, Firewall Events wenn Sie dies in der Firewall Konfiguration für diesen Router aktiviert haben. Für weitere Hinweise schauen Sie im Abschnitt Firewall nach um Firewall Logging zu aktivieren.


Ereignis Protokoll
---------- system log buffer head --------------
Apr 12 14:42:05 home.gateway:ppp:none: Channel Id(0) connected
Apr 12 14:42:05 home.gateway:im_backend:none: Changed ipwan IP address to
80.133.7.204
---------- system log buffer tail --------------
Aktualisieren
Löschen

Fehler Protokoll

Jegliche Fehler die der Router feststellt werden in diesem Fenster gespeichert. (z.B.: ungültige Namenseinträge).

Fehler Protokoll

Fehler Protokoll (*Zeitangabe in Sekunden seit letztem Neustart*)

Wann	Prozess	Fehler Protokoll

NAT Sitzungen

Dieser Abschnitt listet alle aktuellen NAT Sessions zwischen externen (WAN) und internen (LAN) Schnittstellen auf.

NAT Sitzungen

```
   TCP :    2 sessions, Default Timeout   1800 Seconds
   UDP :    0 sessions, Default Timeout    120 Seconds
Others :    0 sessions, Default Timeout     60 Seconds
 Total :    2 sessions
```

Aktualisieren Seite: 1

NAT Sitzungen

```
Active NAT sessions between interface of types external and internal:

No. | Prot | Local IP: Port local/public | Remote IP: Port       | Idle (sec.)
----|------|-----------------------------|-----------------------|-------
1   | TCP  | 192.168.  2.101: 1373/ 1373 | 192.168.  1.254:   80 | 1
2   | TCP  | 192.168.  2.101: 1367/ 1367 | 192.168.  1.254:   80 | 17
```

Aktualisieren Page: 1

Diagnose

Diagnose

LAN Verbindung	
Test Ethernet LAN Verbindung	BESTANDEN
WAN Verbindung	
Test ADSL Synchronisation	BESTANDEN
Test WAN Verbindung	BESTANDEN
Ping Primären Domain Name Server	BESTANDEN
PING www.google.com	BESTANDEN

Aktualisieren

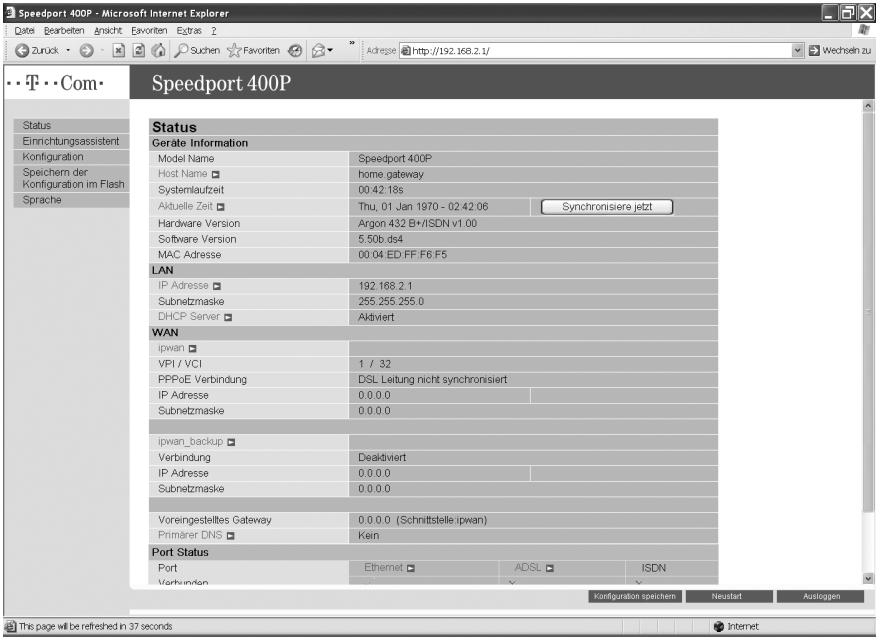
Die Diagnose überprüft die Ethernet-, sowie die WAN-Verbindung. Zusätzlich wird die ADSL Synchronisation überprüft. Sollte einer dieser Tests nicht Bestanden sein überprüfen Sie die Kabelverbindungen. Wenn einer der beiden PING Test fehlschlägt überprüfen Sie Ihre TCP-IP Einstellungen.

UPnP Portmap

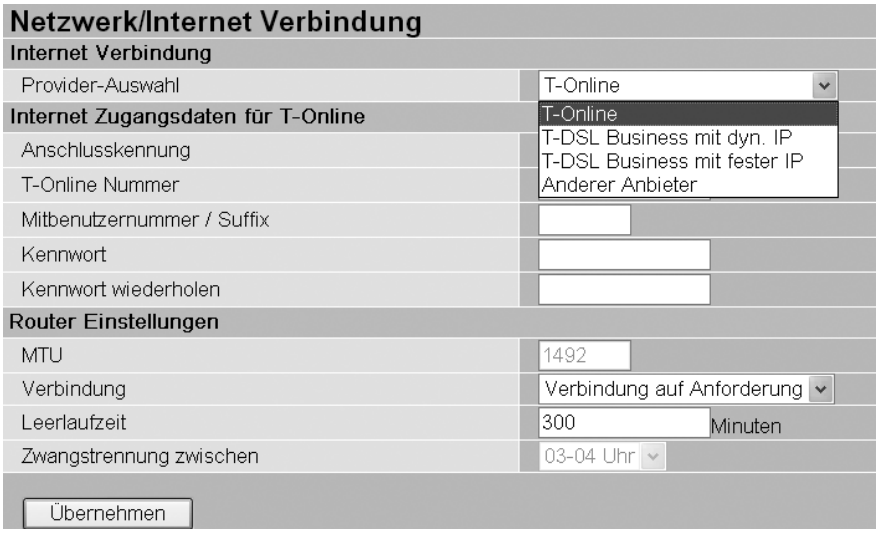
Dieser Abschnitt listet alle Port-mapping Geräte auf, die UPnP (Universal Plug and Play) nutzen. Schlagen Sie im Abschnitt Erweitert in dieser Anleitung nach, um weitere Details für UPnP und die Optionen des Routers für UPnP zu erfahren.

Einrichtungsassistent

Der Einrichtungsassistent hilft Ihnen mit wenigen Schritten die Internetverbindung über ADSL zu erstellen.
Klicken Sie im Menü links auf Einrichtungsassistent.



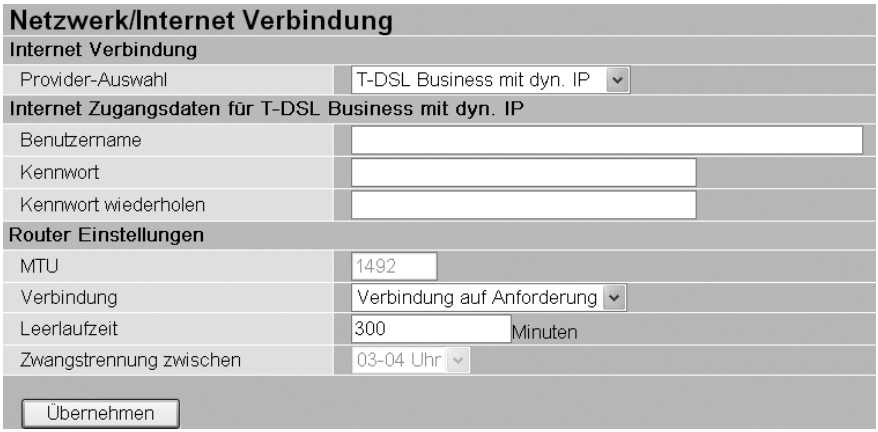
Klicken Sie auf Einrichtungsassistent. Sie können den Provider wählen, den Sie beauftragt haben (T-Online ist voreingestellt, klicken Sie auf den Aufklapp-Pfeil im Menü Provider-Auswahl für weitere Dienstanbieter).



Die Einstellungen für T-Online wurden im Abschnitt Erstkonfiguration erklärt. Folgend werden die Einstellungen der weiteren Dienstanbieter erläutert.

- T-DSL Business mit dynamischer IP
- T-DSL Business mit fester IP
- Anderer Anbieter

T-DSL Business mit dynamischer IP Adresse



Die hier geforderten Daten wurden Ihnen von Ihrem Dienstanbieter in einem Geheimumschlag vorgegeben. Bewahren Sie diese Daten unzugänglich für Unbefugte auf, denn mit diesen Angaben könnten Fremde auf Ihren Namen und auf Ihre Kosten im Internet surfen.

Geben Sie die erforderlichen Dateien ein. Beachten Sie dass Sie das Kennwort zweimal eintragen müssen. Die Eingabe des Kennwort und Kennwort wiederholen wird als Punkte oder Sternchen dargestellt.

Die Angaben unter Router Einstellungen dienen dem Einstellen der Art des Internetzugriffs. Was Sie hier einstellen ist im Besonderen auch davon abhängig, welchen Tarif Sie beauftragt haben.

- Die Grundeinstellung lautet Verbindung auf Anforderung mit einer Leerlaufzeit von 5 Minuten. Die Verbindung zum Internet wird nur aufgebaut wenn Sie z.B. den Browser öffnen oder Emails abrufen. Messenger Programme oder Programme welche ein automatisches Update durchführen veranlassen den Router ebenfalls die Verbindung zum Internet aufzubauen. Nach 5 Minuten ohne Datentransfer wird die Verbindung beendet.

- Aktivieren Sie die Option Ständig verbunden baut der Speedport 400P die Verbindung nicht ab, sondern bleibt immer mit dem Internet verbunden. Zusätzlich können Sie bestimmen wann die Zwangstrennung erfolgen soll.

Wir empfehlen die Option Ständig verbunden nur dann zu aktivieren, wenn Sie über eine Flatrate verfügen. Ansonsten können sehr hohe Kosten anfallen.

Nachdem Sie alle Angaben eingetragen haben, klicken Sie auf Übernehmen.

Klicken Sie auf Konfiguration speichern und bestätigen Sie das Speichern der Konfiguration indem Sie auf Übernehmen klicken.

Wird die Konfiguration nicht gespeichert, werden die Einstellungen bei einem Neustart oder Stromausfall verworfen.

Im Internet surfen

Klicken Sie auf Status. Im Statusfenster unter WAN (Wide Area Network) wird der Status der Internetverbindung (PPPoE Verbindung) angezeigt. Wird Verbindung auf Anforderung aktiviert angezeigt, klicken Sie auf das Symbol Ihres Internet-Browsers. Der Browser wird geöffnet und die für den Browser eingestellte Startseite wird im Internet gesucht und geöffnet. Wird Verbindung hergestellt angezeigt können Sie ebenfalls im Internet surfen. Zusätzlich sehen Sie die aktuelle Verbindungszeit, sowie die Zeit bis zum Auflegen der Verbindung. Die Statusseite wird alle 60 Sekunden aktualisiert.

Möchten Sie eine andere Seite besuchen, z. B. die von T-Online, doppelklicken Sie in die Adresszeile des Browsers, und geben Sie www.t-online.de ein. Drücken Sie anschließend die Enter-Taste. Die Startseite von T-Online wird aufgerufen.

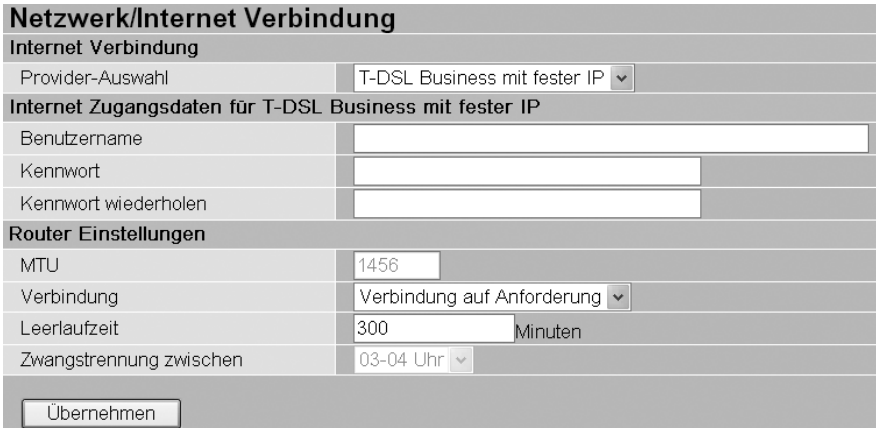
Tipp

Wird das Fenster des erfolgreichen Verbindungsaufbaus nicht in einer Form, die der abgebildeten ähnlich ist, angezeigt, sondern mit einem Fehlerhinweis, konnte keine Verbindung ins Internet hergestellt werden.

Das kann daher rühren, dass

- Sie bei dem angegebenen Dienstanbieter noch nicht angemeldet sind. Rufen Sie die Hotline an und fragen Sie nach.
- Ihnen bei der Eingabe der Daten des Dienstanbieters Fehler unterlaufen sind. Wiederholen Sie die Konfiguration über den Assistenten.
- Die Kabelverbindung zwischen Router und Splitter nicht richtig ist. Prüfen Sie die Verbindungskabel.

T-DSL Business mit fester IP Adresse



Die hier geforderten Daten wurden Ihnen von Ihrem Dienstanbieter in einem Geheimumschlag vorgegeben. Bewahren Sie diese Daten unzugänglich für Unbefugte auf, denn mit diesen Angaben könnten Fremde auf Ihren Namen und auf Ihre Kosten im Internet surfen.

Geben Sie die erforderlichen Dateien ein. Beachten Sie dass Sie das Kennwort zweimal eintragen müssen. Die Eingabe des Kennwort und Kennwort wiederholen wird als Punkte oder Sternchen dargestellt.

Die Angaben unter Router Einstellungen dienen dem Einstellen der Art des Internetzugriffs. Was Sie hier einstellen ist im Besonderen auch davon abhängig, welchen Tarif Sie beauftragt haben.

- Die Grundeinstellung lautet Verbindung auf Anforderung mit einer Leerlaufzeit von 5 Minuten. Die Verbindung zum Internet wird nur aufgebaut wenn Sie z.B. den Browser öffnen oder Emails abrufen. Messenger Programme oder Programme welche ein automatisches Update durchführen veranlassen den Router ebenfalls die Verbindung zum Internet aufzubauen. Nach 5 Minuten ohne Datentransfer wird die Verbindung beendet.

- Aktivieren Sie die Option Ständig verbunden baut der Speedport 400P die Verbindung nicht ab, sondern bleibt immer mit dem Internet verbunden. Zusätzlich können Sie bestimmen wann die Zwangstrennung erfolgen soll.

Wir empfehlen die Option Ständig verbunden nur dann zu aktivieren, wenn Sie über eine Flatrate verfügen. Ansonsten können sehr hohe Kosten anfallen.

Nachdem Sie alle Angaben eingetragen haben, klicken Sie auf Übernehmen.

Klicken Sie auf Konfiguration speichern und bestätigen Sie das Speichern der Konfiguration indem Sie auf Übernehmen klicken.

Wird die Konfiguration nicht gespeichert, werden die Einstellungen bei einem Neustart oder Stromausfall verworfen.

Im Internet surfen

Klicken Sie auf Status. Im Statusfenster unter WAN (Wide Area Network) wird der Status der Internetverbindung (PPPoE Verbindung) angezeigt. Wird Verbindung auf Anforderung aktiviert angezeigt, klicken Sie auf das Symbol Ihres Internet-Browsers. Der Browser wird geöffnet und die für den Browser eingestellte Startseite wird im Internet gesucht und geöffnet. Wird Verbindung hergestellt angezeigt können Sie ebenfalls im Internet surfen. Zusätzlich sehen Sie die aktuelle Verbindungszeit, sowie die Zeit bis zum Auflegen der Verbindung. Die Statusseite wird alle 60 Sekunden aktualisiert.

Möchten Sie eine andere Seite besuchen, z. B. die von T-Online, doppelklicken Sie in die Adresszeile des Browsers, und geben Sie www.t-online.de ein. Drücken Sie anschließend die Enter-Taste. Die Startseite von T-Online wird aufgerufen.

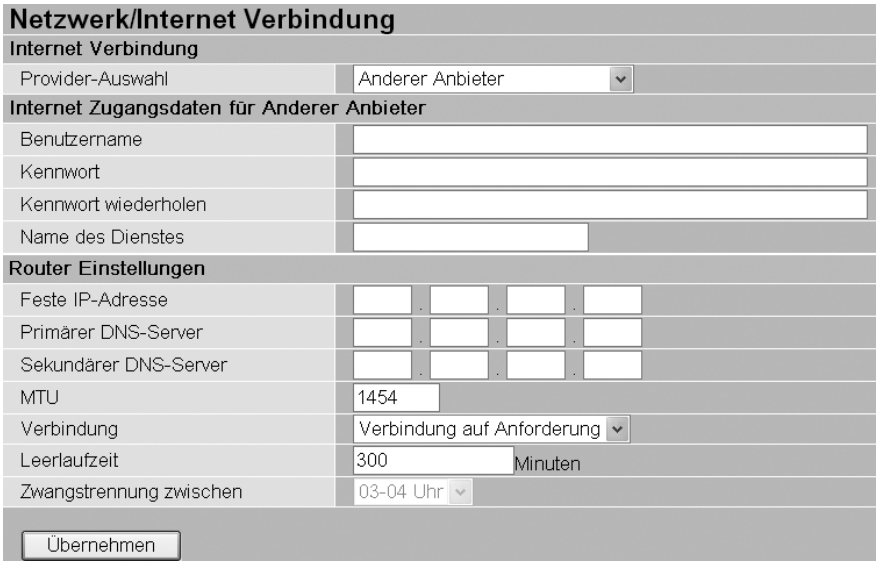
Tipp

Wird das Fenster des erfolgreichen Verbindungsaufbaus nicht in einer Form, die der abgebildeten ähnlich ist, angezeigt, sondern mit einem Fehlerhinweis, konnte keine Verbindung ins Internet hergestellt werden.

Das kann daher rühren, dass

- Sie bei dem angegebenen Dienstanbieter noch nicht angemeldet sind. Rufen Sie die Hotline an und fragen Sie nach.
- Ihnen bei der Eingabe der Daten des Dienstanbieters Fehler unterlaufen sind. Wiederholen Sie die Konfiguration über den Assistenten.
- Die Kabelverbindung zwischen Router und Splitter nicht richtig ist. Prüfen Sie die Verbindungskabel.

Anderer Anbieter



Die hier geforderten Daten wurden Ihnen von Ihrem Dienstanbieter in einem Geheimumschlag vorgegeben. Bewahren Sie diese Daten unzugänglich für Unbefugte auf, denn mit diesen Angaben könnten Fremde auf Ihren Namen und auf Ihre Kosten im Internet surfen.

Geben Sie die erforderlichen Dateien ein. Beachten Sie dass Sie das Kennwort zweimal eintragen müssen. Die Eingabe des Kennwort und Kennwort wiederholen wird als Punkte oder Sternchen dargestellt.

Die Angaben unter Router Einstellungen dienen dem Einstellen der Art des Internetzugriffs. Was Sie hier einstellen ist im Besonderen auch davon abhängig, welchen Tarif Sie beauftragt haben.

- Feste IP-Adresse: Lassen Sie das Feld leer sofern Ihr Dienstanbieter dynamisch eine öffentliche IP Adresse (WAN IP Adresse) für den Router bei jedem Verbindungsaufbau übermittlelt. Haben Sie von Ihrem Dienstanbieter eine feste IP-Adresse erhalten tragen Sie diese hier ein.

- Primärer DNS-Server: Lassen Sie das Feld leer wird die IP Adresse für den primären DNS-Server in der Regel vom Dienstanbieter übermittlelt. Ist dies

nicht der Fall setzen Sie sich mit Ihrem Dienstanbieter in Verbindung, damit Sie eine IP-Adresse für den primären DNS-Server erhalten.

- Sekundärer DNS-Server: Lassen Sie das Feld leer wird die IP Adresse für den sekundären DNS-Server in der Regel vom Dienstanbieter übermittlelt. Ist dies nicht der Fall setzen Sie sich mit Ihrem Dienstanbieter in Verbindung, damit Sie eine IP-Adresse für den sekundären DNS-Server erhalten.

- Das Feld MTU (Maximum Transfer Unit = größte, unfragmentierte Datenmenge bei der Übertragung) ist sehr eng mit dem Übertragungsverfahren des Dienstanbieters verbunden. Verändern Sie den Standardwert nicht, es sei denn, Sie werden von Ihrem Dienstanbieter dazu aufgefordert.

- Die Grundeinstellung lautet Verbindung auf Anforderung mit einer Leerlaufzeit von 5 Minuten. Die Verbindung zum Internet wird nur aufgebaut wenn Sie z.B. den Browser öffnen oder Emails abrufen. Messenger Programme oder Programme welche ein automatisches Update durchführen veranlassen den Router ebenfalls die Verbindung zum Internet aufzubauen. Nach 5 Minuten ohne Datentransfer wird die Verbindung beendet.

- Aktivieren Sie die Option Ständig verbunden baut der Speedport 400P die Verbindung nicht ab, sondern bleibt immer mit dem Internet verbunden. Zusätzlich können Sie bestimmen wann die Zwangstrennung erfolgen soll.

Wir empfehlen die Option Ständig verbunden nur dann zu aktivieren, wenn Sie über eine Flatrate verfügen. Ansonsten können sehr hohe Kosten anfallen.

Nachdem Sie alle Angaben eingetragen haben, klicken Sie auf Übernehmen.

Klicken Sie auf Konfiguration speichern und bestätigen Sie das Speichern der Konfiguration indem Sie auf Übernehmen klicken.

Wird die Konfiguration nicht gespeichert, werden die Einstellungen bei einem Neustart oder Stromausfall verworfen.

Im Internet surfen

Klicken Sie auf Status. Im Statusfenster unter WAN (Wide Area Network) wird der Status der Internetverbindung (PPPoE Verbindung) angezeigt. Wird Verbindung

auf Anforderung aktiviert angezeigt, klicken Sie auf das Symbol Ihres Internet-Browsers. Der Browser wird geöffnet und die für den Browser eingestellte Startseite wird im Internet gesucht und geöffnet. Wird Verbindung hergestellt angezeigt können Sie ebenfalls im Internet surfen. Zusätzlich sehen Sie die aktuelle Verbindungszeit, sowie die Zeit bis zum Auflegen der Verbindung. Die Statusseite wird alle 60 Sekunden aktualisiert.

Möchten Sie eine andere Seite besuchen, z. B. die von T-Online, doppelklicken Sie in die Adresszeile des Browsers, und geben Sie www.t-online.de ein. Drücken Sie anschließend die Enter-Taste. Die Startseite von T-Online wird aufgerufen.

Tipp

Wird das Fenster des erfolgreichen Verbindungsaufbaus nicht in einer Form, die der abgebildeten ähnlich ist, angezeigt, sondern mit einem Fehlerhinweis, konnte keine Verbindung ins Internet hergestellt werden.

Das kann daher rühren, dass

- Sie bei dem angegebenen Dienstanbieter noch nicht angemeldet sind. Rufen Sie die Hotline an und fragen Sie nach.

- Ihnen bei der Eingabe der Daten des Dienstanbieters Fehler unterlaufen sind. Wiederholen Sie die Konfiguration über den Assistenten.

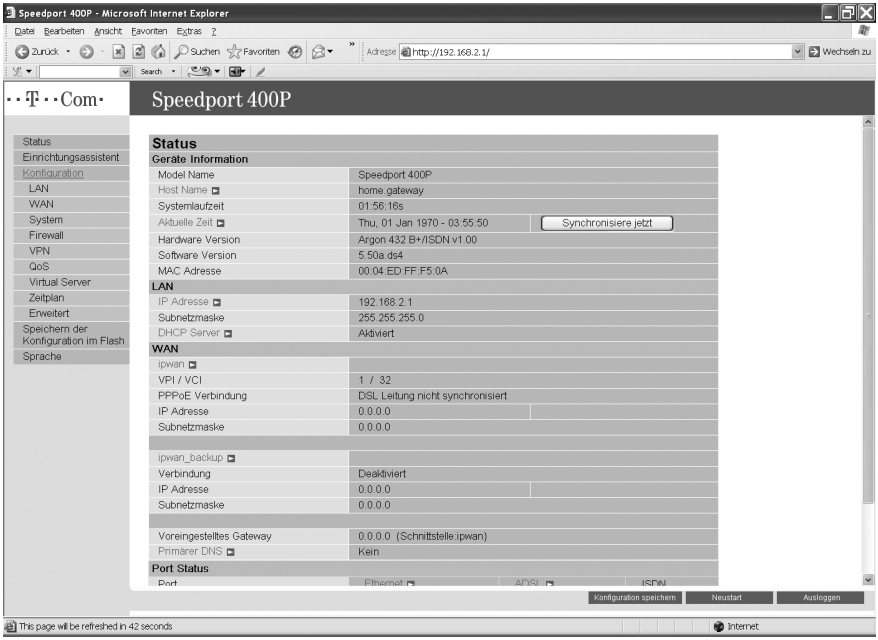
- Die Kabelverbindung zwischen Router und Splitter nicht richtig ist. Prüfen Sie die Verbindungskabel.

Konfiguration

Wenn Sie dieses Feld anklicken, erhalten Sie folgendes Untermenü, um den Router zu konfigurieren.

LAN, WAN, System, Firewall, VPN, QoS, Virtual Server, Zeitplan und Erweitert

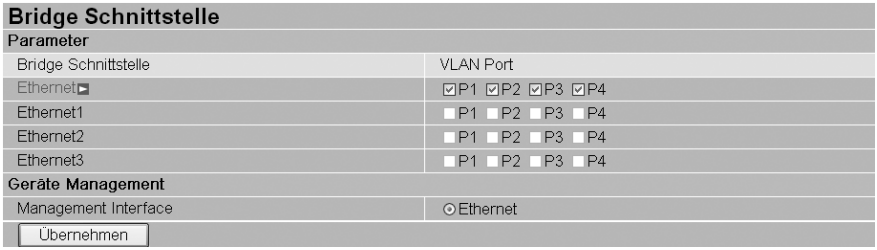
Diese Funktionen werden im Folgenden beschrieben



LAN (Local Area Network)

Es gibt fünf Unterpunkte im Menü LAN: **Bridge Schnittstelle, Ethernet, Ethernet Client Filter, Port Einstellungen** und **DHCP Server.**

Bridge Schnittstelle



- Sie können Mitglieder Ports für jede VLAN Gruppe in der Bridge Schnittstellen Sektion einstellen. Im Beispiel werden zwei VLAN Gruppen erstellt.
- Ethernet: P1 (Port 1)
- Ethernet1: P2 und P3 (Port 2, 3) Bitte deaktivieren Sie zuerst P2, P3 vom Ethernet VLAN und aktivieren diese dann unter Ethernet1.

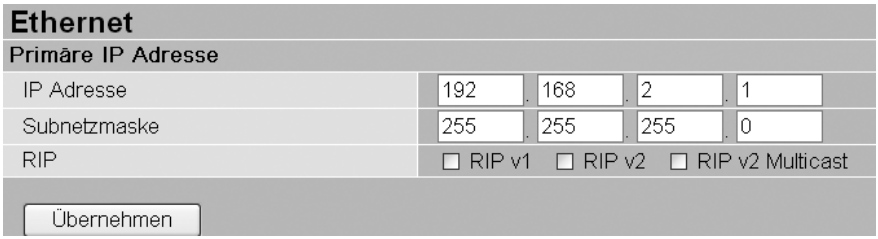
Hinweis: Sie sollten jede VLAN Gruppe behutsam einstellen. Jede Bridge Schnittstelle ist wie folgt zugeordnet.

Bridge Schnittstelle	VLAN Port (Startet immer mit)
Ethernet	P1 / P2 / P3
Ethernet1	P2 / P3
Ethernet2	P3

Management Schnittstelle: Hier geben Sie an welche VLAN Gruppe den Router verwalten darf.

Hinweis: NAT/NAPT kann nur an der Managementschnittstelle angewendet werden.

Ethernet



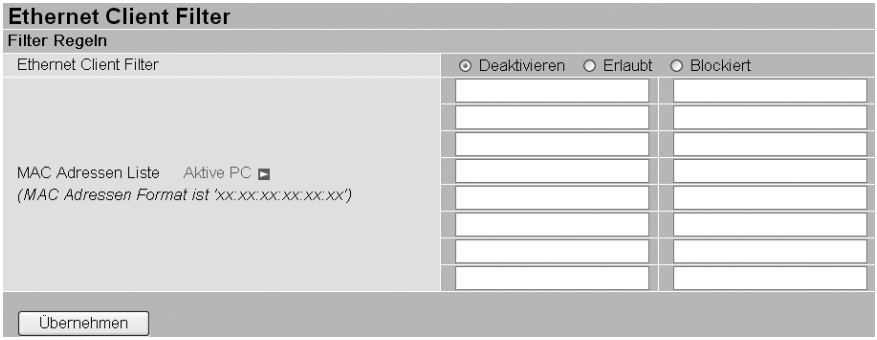
Es werden zwei Ethernet IP-Adressen im LAN unterstützt. Mit dieser Funktion kann der Router zwei unterschiedliche LAN Teilnetze bei gleichzeitigem Internetzugriff unterstützen. Normalerweise existiert nur ein Teilnetz im LAN, so dass keine Notwendigkeit besteht die zweite IP-Adresse zu konfigurieren. 192.168.2.1 ist die voreingestellte IP-Adresse dieses Routers.

RIP:

RIP v1, RIP v2, und RIP v2 Multicast. Klicken Sie um die RIP Funktionen zu verwenden.

Ethernet Client Filter

Der Ethernet Client Filter unterstützt bis zu 16 Ethernet Geräte anhand der MAC Adresse. Dies hilft Ihnen Ihr Netzwerk zu administrieren bzw. zu kontrollieren, damit nur bestimmte Geräte Ihr LAN nutzen bzw. nicht nutzen dürfen.
Es gibt keine Voreinstellungen. Sie bestimmen die Filter Regeln nach Ihren Ansprüchen.



Ethernet Client Filter:

In der Werkseinstellung sind die Filter deaktiviert.

- Erlaubt: Klicken damit authorisierte Geräte Zugriff auf Ihr LAN erhalten, indem Sie die MAC Adresse eintragen oder Sie klicken auf Aktive PC . Vergewissern Sie sich das Ihr PC mit der MAC Adresse gelistet ist.

- Blockiert: Klicken damit nicht authorisierte Geräte keinen Zugriff auf Ihr LAN erhalten, indem Sie die MAC Adresse eintragen oder Sie klicken auf Aktive PC . Vergewissern Sie sich das Ihr PC mit der MAC Adresse nicht gelistet ist.

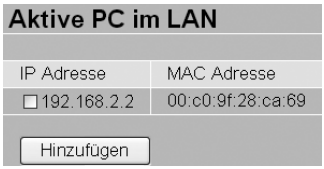
Die maximale Anzahl beträgt 16 Clients. Die MAC Adressen sind 6 Bytes lang und nur im Hexadezimalen Format angegeben. Die Zahlen **0 - 9** und Buchstaben **a - f** werden akzeptiert.

Hinweis: Folgen Sie diesem MAC Adressen Format xx:xx:xx:xx:xx:xx. Doppelpunkt (:) muss angegeben werden.

Aktive PC:

Geräte welche über Ethernet mit dem Router verbunden sind werden hier automatisch angezeigt.

Aktive PC → Aktive PC im LAN

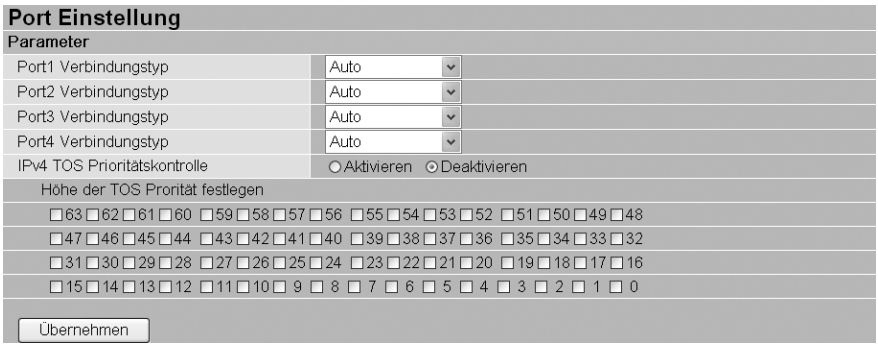


Active PC im LAN zeigt die Liste der Ethernet Geräte mit IP und MAC Adresse welche mit dem Router verbunden sind.

Klicken Sie einfach auf die Box neben der IP Adresse damit das Gerät blockiert bzw. die Erlaubnis für den Zugriff zum LAN erhält. Dann auf Hinzufügen. Maximal 16 Einträge.

Port Einstellungen

Dieser Abschnitt erlaubt Ihnen die Einstellungen der Ethernet Ports des Routers zu konfigurieren um eventuell vorhandene Kompatibilitätsprobleme die unter Umständen bei der Verbindung mit dem Internet auftreten zu beheben. Benutzer können zusätzlich die Performance Ihres Netzwerkes optimieren.


Port Einstellung
Parameter
Port1 Verbindungstyp
Auto
Port2 Verbindungstyp
Auto
Port3 Verbindungstyp
Auto
Port4 Verbindungstyp
Auto
IPv4 TOS Prioritätskontrolle
Aktivieren
Deaktivieren
Höhe der TOS Prorität festlegen
63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48
47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Übernehmen

Port # Verbindungstyp:

Fünf Optionen stehen zur Auswahl: Auto, 10M half-duplex, 10M full-duplex, 100M half-duplex order 100M full-duplex. Manchmal gibt es Ethernet Kompatibilitätsprobleme mit alten Ethernet Geräten und Sie können verschiedene Geschwindigkeiten konfigurieren um diese Probleme zu lösen. Werksseitig ist **Auto** eingestellt. Sie sollten diese Einstellung belassen sofern keine Problem mit PCs auftreten, welche keinen Zugriff auf das Internet haben.

IPv4 TOS Prioritätskontrolle (für erfahrene Anwender):

TOS, Type Of Services, ist das zweite Oktett eines IP Paketes. Bits 6-7 dieses Oktetts sind reserviert und Bit 0-5 werden verwendet um die Priorität des Paketes festzulegen.

Diese Feature verwendet die Bits 0-5 um die Paket-Priorität zu klassifizieren. Wenn das Paket eine hohe Priorität hat wird dieses zuerst bearbeitet und ist nicht abhängig von einer Limitierung. Daher, wenn dieses Feature aktiviert ist, überprüft der Ethernet Switch des Routers das zweite Oktett jedes einzelnen IP Paketes. Wenn der Wert im TOS Feld mit den aktivierten Werten übereinstimmt (0 bis 63), wird dieses Paket mit hoher Priorität behandelt.

DHCP Server

Sie können DHCP (Dynamic Host Configuration Protocol) aktivieren oder deaktivieren oder die DHCP Relay Funktion aktivieren. Das DHCP Protokoll erlaubt Ihrem Router dynamische IP Adressen an die PCs zu verteilen, sofern diese so konfiguriert sind

DHCP Server	
Konfiguration	
DHCP Server Modus	○ Deaktiviert ◉ DHCP Server ○ DHCP Relay Agent
Weiter	

DHCP Server Status	
Erlaube Bootp	wahr
Erlaube unbekannte Clients	wahr
Aktivieren	wahr
Subnetz Definitionen	
Subnetz Wert	192.168.2.0
Subnetzmaske	255.255.255.0
Maximale Lease Zeit	86400 Sekunden
Voreingestellte Lease Zeit	43200 Sekunden
Benutze lokale Host Adresse als DNS Server	wahr
Benutze lokale Host Adresse als voreingestelltes Gateway	wahr
Beziehe Subnetz von der IP-Schnittstelle	iplan
IP Bereich *192.168.2.100- 192.168.2.199*	
Option *domain-name-servers= 0.0.0.0*	

Damit die DHCP Serverfunktion deaktiviert wird, wählen Sie Deaktivieren und klicken Weiter, dann klicken Sie Übernehmen. Jedem PC im LAN sollte eine feste IP-Adresse zugewiesen werden, sowie das Standard Gateway des Routers (Standardmäßig ist dies 192.168.2.1).

Wenn Sie DHCP Server auswählen und auf Weiter klicken, dann können Sie die Parameter des DHCP Servers konfigurieren, wie IP Pool (Anfangs IP-Adresse und Ende IP-Adresse), leased time für jede zugewiesene IP-Adresse, DNS IP-Adresse und Gateway IP-Adresse. Diese Nachrichten werden an den DHCP

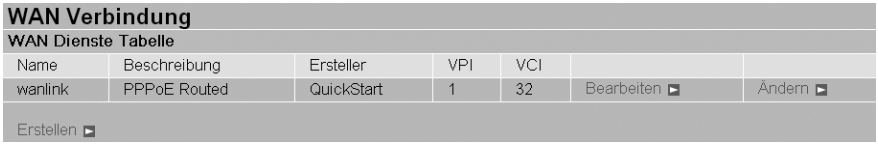
Client gesendet, wenn er eine IP-Adresse vom DHCP Server anfordert. Klicken Sie Übernehmen, um diese Funktion zu aktivieren. Wenn Sie „Benutze Router als DNS Server“ auswählen, findet der Router die IP-Adresse automatisch vom äußeren Netzwerk und leitet sie weiter an den anfordernden PC im LAN.

Wenn Sie DHCP Relay Agent wählen und auf „Weiter“ klicken, dann müssen Sie die IP-Adresse des DHCP Servers eingeben, der die zugewiesene IP-Adresse an den DHCP Client im LAN weiter gibt. Benutzen Sie diese Funktion nur wenn Sie von Ihrem Netzwerk Administrator oder ISP so angewiesen werden.
Klicken Sie auf „Übernehmen“ um die Funktion zu aktivieren.

WAN (Wide Area Network)

WAN beschreibt Ihre Wide Area Network Verbindung, z.B. die Verbindung vom Router zu Ihrem ISP und dem Internet. Es gibt vier Unterpunkte im Menü WAN: **ISP, Backup ISP, DNS** und **ADSL.**

ISP



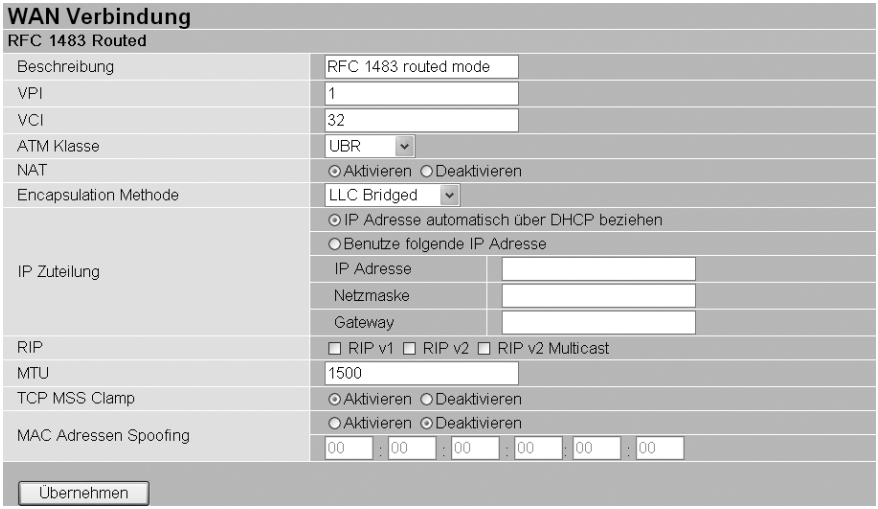
Die Werkseinstellung ist PPPoE. Wenn Ihr ISP das gleiche Protokoll verwendet, klicken Sie Bearbeiten, um weitere Eingaben wie folgt vorzunehmen. Wenn Ihr ISP PPPoE nicht unterstützt, dann klicken Sie auf Bearbeiten. Dann können Sie Erstellen anklicken, um eine neue Verbindung zu Ihrem ISP zu erstellen.

Eine einfache Alternative ist den Einrichtungsassistenten vom Hauptmenü auf der linken Seite auszuwählen. Bitte sehen Sie im Abschnitt Einrichtungsassist nach für weitere Informationen.

Weitere Informationen der verschiedenen Protokolle finden Sie in der folgenden Tabelle. Am verbreitesten ist das PPPoE Protokoll.

Merkmal	Beschreibung
PPPoE (Point to Point over Ethernet)	VPI/VCI, VC-basiertes/LLC-basiertes Multiplexing, Benutzername, Passwort, Service Name, und Domain Name System (DNS) IP-Adresse (diese kann vom ISP zugewiesen werden oder fest sein)
PPPoA (Point to Point over ATM)	VPI/VCI, VC-basiertes/LLC-basiertes Multiplexing, Benutzername, Passwort und Domain Name System (DNS) IP-Adresse (diese kann vom ISP zugewiesen werden oder fest sein)
RFC1483 Bridged	VPI/VCI, VC-basiertes/LLC-basiertes Multiplexing die Verwendung des Router im einfachen Modem Modus (keine Router Funktionen verfügbar)
RFC1483 Routed	VPI/VCI, VC-basiertes/LLC-basiertes Multiplexing, IP-Adresse, Teilnetz-Maske, Gateway Adresse, und Domain Name System (DNS) IP-Adresse (es ist eine feste IP-Adresse)
IPoA (Internet Protocol over ATM)	VPI/VCI, IP-Adresse, Teilnetz-Maske, Gateway Adresse, und Domain Name System (DNS) IP-Adresse (es ist eine feste IP-Adresse)

RFC 1483 Routed Verbindungen



Beschreibung:

Ihre Beschreibung für diese Verbindung.

VPI und VCI:

Geben Sie diese Information so ein wie von Ihrem ISP vorgegeben.

ATM Klasse:

Die “Quality of Service” für den ATM Layer.

NAT:

NAT erlaubt mehreren Nutzern mit einem einzigen IP-Account und einer einzigen IP-Adresse Zugang zum Internet. Falls LAN-User öffentliche IP-Adressen haben und direkt auf das Internet zugreifen, kann NAT abgeschaltet werden.

Encapsulation Methode:

Wählen Sie das Protokoll, welches von Ihrem ISP vorgeben ist. Voreingestellt ist LLC Bridged.

DHCP Client:

Aktivieren oder deaktivieren Sie den DHCP Client. Spezifizieren Sie, ob der Router vom Internet Service Provider (ISP) eine automatische IP-Adresse zugewiesen bekommen kann oder nicht.

Bitte klicken Sie „IP-Adresse automatisch über DHCP beziehen“ an, um den DHCP Client zu aktivieren oder klicken Sie „Benutze folgende IP Adresse“ um den DHCP Client zu deaktivieren und spezifizieren Sie die IP-Adresse manuell. Diese Einstellungen werden von Ihrem ISP vorgegeben.

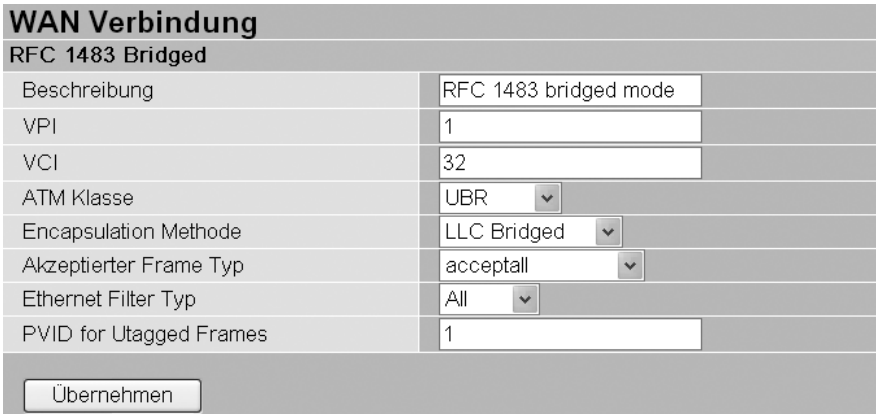
RIP:

RIP v1, RIP v2, und RIP v2 Multicast. Wählen Sie dies aus, um die RIP Funktion zu aktivieren.

MTU:

Maximum Transmission Unit. Die Größe des größten Datagramms (ohne media-spezifische Header) welche IP durch das Interface hindurchsenden wird.

RFC 1483 Bridged Verbindungen



VPI und VCI:

Geben Sie diese Information so ein wie von Ihrem ISP vorgegeben.

ATM Klasse:

Die “Quality of Service” für den ATM Layer.

Encapsulation Methode:

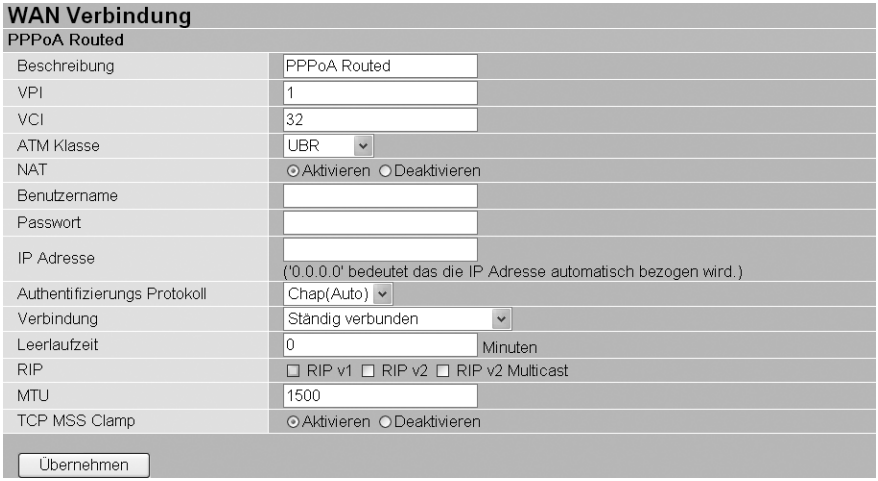
Wählen Sie das Protokoll, welches von Ihrem ISP vorgeben ist. Voreingestellt ist LLC Bridged.

Ethernet Filter Typ:

Geben Sie den Ethernet Filter für die Bridge Schnittstelle an.

Ethernet Filter Typ	
All	Erlaubt alle Typen von Ethernet Pakete durch den Port.
Ip	Erlaubt nur IP/ARP Typen von Ethernet Paketen durch den Port.
PPPoE	Erlaubt nur PPPoE Typen von Ethernet Paketen durch den Port.

PPPoA Routed Verbindungen



Beschreibung:

Ihre Beschreibung für diese Verbindung.

VPI und VCI:

Geben Sie diese Information so ein wie von Ihrem ISP vorgegeben.

ATM Klasse:

Der Quality of Service für den ATM Layer.

NAT:

NAT erlaubt mehreren Nutzern mit einem einzigen IP-Account und einer einzigen IP-Adresse Zugang zum Internet. Falls LAN-User öffentliche IP-Adressen haben und direkt auf das Internet zugreifen, kann NAT abgeschaltet werden.

Benutzername:

Geben Sie Ihren Benutzernamen ein, den Sie von Ihrem Provider erhalten haben. Sie können bis zu 128 alphanumerische Zeichen eingeben (Groß- und Kleinschreibung beachten). Sehr oft in der Form „benutzername@ispname“ anstelle “Benutzername”.

Passwort:

Geben Sie das zu dem Benutzernamen gehörende Passwort ein.

Sie können bis zu 128 alphanumerische Zeichen eingeben (Gross- und Kleinschreibung beachten).

IP Adresse:

Spezifiziert ob der Router eine IP Adresse von Internet Service Provider (ISP) automatisch erhält oder nicht. Diese Angaben sind abhängig von Ihrem ISP.

Authentifizierungs Protokoll:

Standard ist Chap(Auto). Ihr ISP wird Ihnen mitteilen ob Sie alternativ Chap oder Pap benutzen sollen.

Verbindung:

- **Ständig verbunden:**
  Wenn Sie möchten, das der Router eine PPPoA Sitzung startet sobald er an ist und diese nach Verbindungsabbruch durch den ISP automatisch wieder aufbaut (z.B. Zwangstrennung).

- **Verbindung auf Anforderung:**
  Wenn Sie eine PPPoA Sitzung nur dann möchten, wenn ein Paket Zugang zum Internet verlangt (z.B.: wenn ein Programm auf Ihrem Computer Zugriff zum Internet verlangt).

Leerlaufzeit:

Automatischer Verbindungsabbau des Router wenn keine Aktivität für eine voreingestellte Zeit stattfindet.

- **Details:** Hier können Sie die Ziel Ports und die Paket Typen angeben (TCP/UDP) welche von der Leerlaufzeit nicht überprüft werden. Dies erlaubt Ihnen anzugeben welcher nach außen gehende Datenverkehr die Leerlaufzeit nicht auslöst.

RIP:

RIP v1, RIP v2, und RIP v2 Multicast. Wählen Sie dies aus, um die RIP Funktion zu aktivieren.

MTU:

Maximum Transmission Unit. Die Größe des größten Datagramms (ohne media-spezifische Header) welche IP durch das Interface hindurchsenden wird.

Erweiterte Optionen (PPPoA)

LLC Header:

Wählt den Encapsulation Modus aus, true für LLC bzw. false für VC-Mux.

Route erstellen:

Diese Einstellung gibt an ob eine Route zum System hinzugefügt wird nachdem die IPCP (Internet Protocol Control Protocol) Verhandlung beendet ist. Wenn dies wahr ist, wird eine Route angelegt, welche Pakete direkt an das Remote Ende des PPP Link leitet.

Spezielle Route:

Gibt an ob eine Route angelegt wird wenn ein PPP Link eine gezielte oder Standard-Route ist. Wenn dies wahr ist, wird die Route nur für Pakete gültig sein für das Subnetz am Remote Ende des PPP Link. Die Adresse dieses Subnetz wird während der IPCP Verhandlung bezogen.

Subnet Maske:

Stellt die Subnetz Maske, die für das lokale IP Interface zum PPP Transport verwendet wird zur Verfügung. Wenn die Angabe 0.0.0.0 ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet.

Route Maske:

Stellt die Subnetz Maske, die für die Route benutzt wird, wenn ein PPP Link aufkommt, zur Verfügung. Wenn die Angabe 0.0.0.0 ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet.

MRU:

Maximum Receive Unit. Dies wird vereinbart während der LCP Protokoll Phase.

Finde Primären / Sekundären DNS:

Diese Einstellung aktiviert / deaktiviert ob die primäre/sekundäre DNS Server Adresse vom Remote PPP Peer über IPCP angefragt wird. Die Standardeinstellung hierbei ist „wahr“.

Übergebe DNS an Relay:

Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen Remote Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an das lokale DNS Relay weitergeben, so dass die Verbindung aufgebaut werden kann.

Übergebe DNS an Client:

Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen Remote Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an die lokalen Clients weitergeben, so dass die Verbindung aufgebaut werden kann.

Übergebe DNS an DHCP Server:

Ähnlich wie oben, aber gibt die DNS Server Adresse an den DHCP Server weiter.

Finde Primären NBNS / Sekundären NBNS:

Diese Einstellung aktiviert / deaktiviert ob die primäre / sekundäre NBNS Server Adresse vom Remote Peer über IPCP angefragt wird. Der Standardwert dafür ist „falsch“.

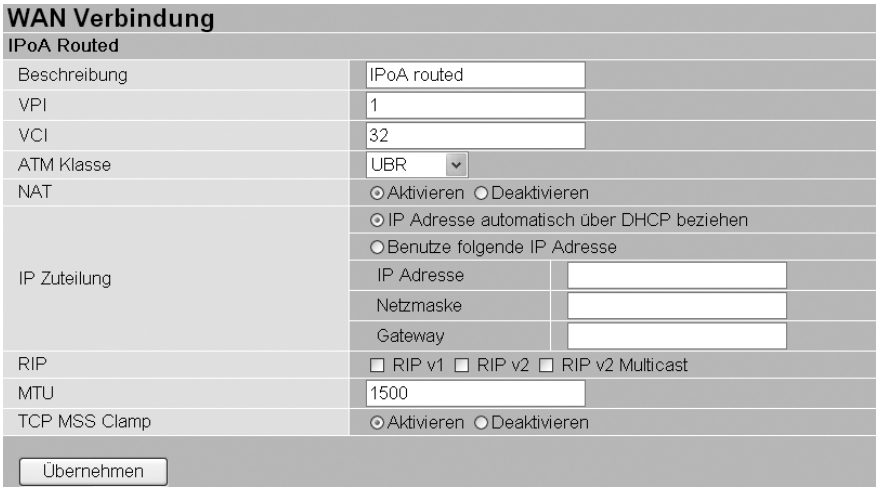
Finde Subnet Maske:

Gibt an, ob die Subnetzmaske während der IPCP Verhandlung benutzt wird oder nicht.

Übergebe Subnet Maske an DHCP Server:

Aktiviert um Ihre DHCP Server Einstellungen zu verändern mit den Informationen die Sie während des IPCP Verhandlung erhalten.

IPoA Routed Verbindungen



Beschreibung:

Ihre Beschreibung für diese Verbindung.

VPI und VCI:

Geben Sie diese Information so ein wie von Ihrem ISP vorgegeben.

ATM Klasse:

Der Quality of Service für den ATM Layer.

NAT:

NAT erlaubt mehreren Nutzern mit einem einzigen IP-Account und einer einzigen IP-Adresse Zugang zum Internet. Falls LAN-User öffentliche IP-Adressen haben und direkt auf das Internet zugreifen, kann NAT abgeschaltet werden.

DHCP Client:

Aktivieren oder deaktivieren Sie den DHCP Client. Spezifizieren Sie, ob der Router vom Internet Service Provider (ISP) eine automatische IP-Adresse zugewiesen bekommen kann oder nicht. Bitte klicken Sie „IP-Adresse automatisch über DHCP beziehen“ an, um den DHCP Client zu aktivieren oder klicken Sie „Benutze folgende IP Adresse“ um den DHCP Client zu deaktivieren und spezifizieren Sie die IP-Adresse manuell. Diese Einstellungen werden von Ihrem ISP vorgegeben.

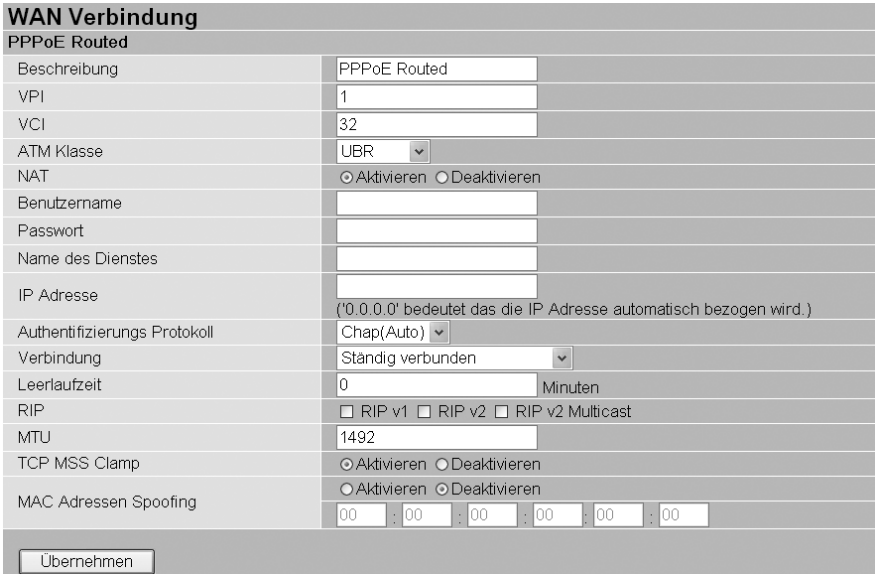
RIP:

RIP v1, RIP v2, und RIP v2 Multicast. Wählen Sie dies aus, um die RIP Funktion zu aktivieren.

MTU:

Maximum Transmission Unit. Die Größe des größten Datagramm (ohne media-spezifische Header) welche IP durch das Interface hindurchsenden wird.

PPPoE Verbindungen



Beschreibung:

Ihre Beschreibung für diese Verbindung.

VPI und VCI:

Geben Sie diese Information so ein wie von Ihrem ISP vorgegeben.

ATM Klasse:

Der Quality of Service für den ATM Layer.

NAT:

NAT erlaubt mehreren Nutzern mit einem einzigen IP-Account und einer einzigen IP-Adresse Zugang zum Internet. Falls LAN-User

öffentliche IP-Adressen haben und direkt auf das Internet zugreifen, kann NAT abgeschaltet werden.

Benutzername:

Geben Sie Ihren Benutzernamen ein, den Sie von Ihrem Provider erhalten haben. Sie können bis zu 128 alphanumerische Zeichen eingeben (Gross- und Kleinschreibung beachten). Sehr oft in der Form „benutzername@ispname“ anstelle “Benutzername”.

Passwort:

Geben Sie das zu dem Benutzernamen gehörende Passwort ein. Sie können bis zu 128 alphanumerische Zeichen eingeben (Gross- und Kleinschreibung beachten).

Dienst Name:

Dieser Punkt ist nur zur Identifizierung gedacht. Wenn benötigt, wird Ihnen Ihr ISP weitere Informationen mitteilen. Maximal können Sie 20 alphanumerische Zeichen eingeben.

IP Adresse:

Spezifiziert ob der Router eine IP Adresse von Internet Service Provider (ISP) automatisch erhält oder nicht. Diese Angaben sind abhängig von Ihrem ISP.

Authentifizierungs Protokoll:

Standard ist Chap(Auto). Ihr ISP wird Ihnen mitteilen ob Sie alternativ Chap oder Pap benutzen sollen.

Verbindung:

- Ständig verbunden: Wenn Sie möchten, das der Router eine PPPoE Sitzung startet sobald er an ist und diese nach Verbindungsabbruch durch den ISP automatisch wieder aufbaut (z.B. Zwangstrennung).

- Verbindung auf Anforderung: Wenn Sie eine PPPoE Sitzung nur dann möchten, wenn ein Paket Zugang zum Internet verlangt (z.B.: wenn ein Programm auf Ihrem Computer Zugriff zum Internet verlangt).

Leerlaufzeit:

Automatischer Verbindungsabbau des Router wenn keine Aktivität für eine voreingestellte Zeit stattfindet.

- Details: Hier können Sie die Ziel Ports und die Paket Typen angeben (TCP/UDP) welche von der Leerlaufzeit nicht überprüft werden. Dies erlaubt Ihnen anzugeben welcher nach außen gehende Datenverkehr die Leerlaufzeit nicht auslöst.

RIP:

RIP v1, RIP v2, und RIP v2 Multicast. Wählen Sie dies aus, um die RIP Funktion zu aktivieren.

MTU:

Maximum Transmission Unit. Die Größe des größten Datagramm (ohne media-spezifische Header) welche IP durch das Interface hindurchsenden wird.

Erweiterte Optionen (PPPoE)

LLC Header:

Wählt den Encapsulation Modus aus, true für LLC bzw. false für VC-Mux.

Route erstellen:

Diese Einstellung gibt an ob eine Route zum System hinzugefügt wird nachdem die IPCP (Internet Protocol Control Protocol) Verhandlung beendet ist. Wenn dies wahr ist, wird eine Route angelegt, welche Pakete direkt an das Remote Ende des PPP Link leitet.

Spezielle Route:

Gibt an ob eine Route angelegt wird wenn ein PPP Link eine gezielte oder Standard-Route ist. Wenn dies wahr ist, wird die Route nur für Pakete gültig sein für das Subnetz am Remote Ende des PPP Link. Die Adresse dieses Subnetz wird während der IPCP Verhandlung bezogen.

Subnet Maske:

Stellt die Subnetz Maske, die für das lokale IP Interface zum PPP Transport verwendet wird zur Verfügung. Wenn die Angabe 0.0.0.0

ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet.

Route Maske:

Stellt die Subnetz Maske, die für die Route benutzt wird, wenn ein PPP Link aufkommt, zur Verfügung. Wenn die Angabe 0.0.0.0 ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet.

MRU:

Maximum Receive Unit. Dies wird vereinbart während der LCP Protokoll Phase.

Finde Primären / Sekundären DNS:

Diese Einstellung aktiviert / deaktiviert ob die primäre/sekundäre DNS Server Adresse vom Remote PPP Peer über IPCP angefragt wird. Die Standardeinstellung hierbei ist „wahr".

Übergebe DNS an Relay:

Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen Remote Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an das lokale DNS Relay weitergeben so das die Verbindung aufgebaut werden kann.

Übergebe DNS an Client:

Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen Remote Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an die lokalen Clients weitergeben so das die Verbindung aufgebaut werden kann.

Übergebe DNS an DHCP Server:

Ähnlich wie oben, aber gibt die DNS Server Adresse an den DHCP Server weiter.

Finde Primären NBNS / Sekundären NBNS:

Diese Einstellung aktiviert / deaktiviert ob die primäre / sekundäre NBNS Server Adresse vom Remote Peer über IPCP angefragt wird. Der Standardwert dafür ist „falsch".

Finde Subnet Maske:

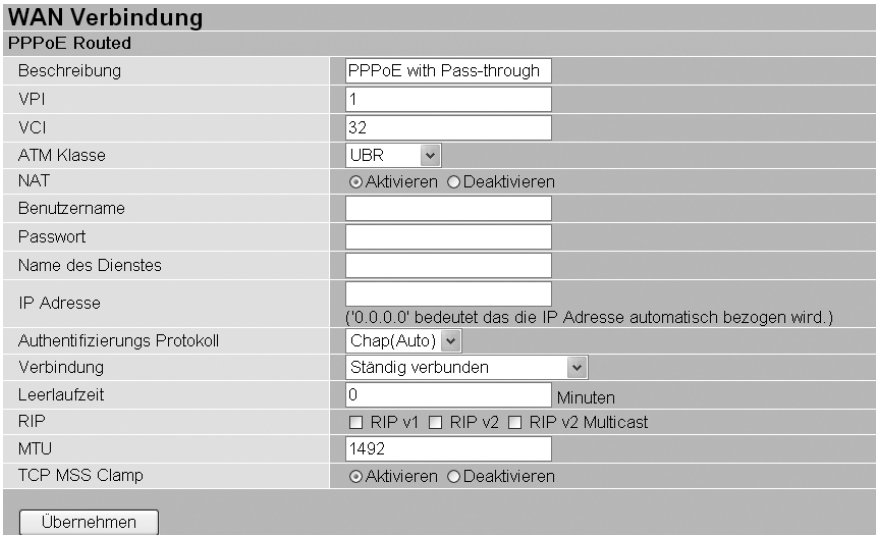
Gibt an, ob die Subnetzmaske während der IPCP Verhandlung benutzt wird oder nicht.

Übergebe Subnet Maske an DHCP Server:

Aktiviert um Ihre DHCP Server Einstellungen zu verändern mit den Informationen die Sie während des IPCP Verhandlung erhalten.

PPPoE mit Pass-through Verbindungen

Die Funktion PPPoE mit Pass-through Verbinden erhalten Sie über den Konfigurator. Klicken Sie auf Konfiguration ➜ WAN ➜ ISP ➜ ÄNDERN.



Beschreibung:

Ihre Beschreibung für diese Verbindung.

VPI und VCI:

Geben Sie diese Information so ein wie von Ihrem ISP vorgegeben.

ATM Klasse:

Der Quality of Service für den ATM Layer.

NAT:

NAT erlaubt mehreren Nutzern mit einem einzigen IP-Account und einer einzigen IP-Adresse Zugang zum Internet. Falls LAN-User öffentliche IP-Adressen haben und direkt auf das Internet zugreifen, kann NAT abgeschaltet werden.

Benutzername:

Geben Sie Ihren Benutzernamen ein, den Sie von Ihrem Provider erhalten haben. Sie können bis zu 128 alphanumerische Zeichen

eingeben (Gross- und Kleinschreibung beachten). Sehr oft in der Form „benutzername@ispname“ anstelle “Benutzername”.

Passwort:

Geben Sie das zu dem Benutzernamen gehörende Passwort ein. Sie können bis zu 128 alphanumerische Zeichen eingeben (Gross- und Kleinschreibung beachten).

Dienst Name:

Dieser Punkt ist nur zur Identifizierung gedacht. Wenn benötigt, wird Ihnen Ihr ISP weitere Informationen mitteilen. Maximal können Sie 20 alphanumerische Zeichen eingeben.

IP Adresse:

Spezifiziert ob der Router eine IP Adresse von Internet Service Provider (ISP) automatisch erhält oder nicht. Diese Angaben sind abhängig von Ihrem ISP.

Authentifizierungs Protokoll:

Standard ist Chap(Auto). Ihr ISP wird Ihnen mitteilen ob Sie alternativ Chap oder Pap benutzen sollen.

Verbindung:

- Ständig verbunden: Wenn Sie möchten, das der Router eine PPPoE Sitzung startet sobald er an ist und diese nach Verbindungsabbruch durch den ISP automatisch wieder aufbaut (z.B. Zwangstrennung).

- Verbindung auf Anforderung: Wenn Sie eine PPPoE Sitzung nur dann möchten, wenn ein Paket Zugang zum Internet verlangt (z.B.: wenn ein Programm auf Ihrem Computer Zugriff zum Internet verlangt).

Leerlaufzeit: Automatischer Verbindungsabbau des Router wenn keine Aktivität für eine voreingestellte Zeit stattfindet.

- Details: Hier können Sie die Ziel Ports und die Paket Typen angeben (TCP/UDP) welche von der Lerlaufzeit nicht überprüft werden. Dies erlaubt Ihnen anzugeben welcher nach außen gehende Datenverkehr die Leerlaufzeit nicht auslöst.

RIP:

RIP v1, RIP v2, und RIP v2 Multicast. Wählen Sie dies aus, um die RIP Funktion zu aktivieren.

MTU:

Maximum Transmission Unit. Die Größe des größten Datagramm (ohne media-spezifische Header) welche IP durch das Interface hindurchsenden wird.

Erweiterte Optionen (PPPoE)

LLC Header:

Wählt den Encapsulation Modus aus, true für LLC bzw. false für VC-Mux.

Route erstellen:

Diese Einstellung gibt an ob eine Route zum System hinzugefügt wird nachdem die IPCP (Internet Protocol Control Protocol) Verhandlung beendet ist. Wenn dies wahr ist, wird eine Route angelegt, welche Pakete direkt an das Remote Ende des PPP Link leitet.

Spezielle Route:

Gibt an ob eine Route angelegt wird wenn ein PPP Link eine gezielte oder Standard Route ist. Wenn dies wahr ist, wird die Route nur für Pakete gültig sein für das Subnetz am Remote Ende des PPP Link. Die Adresse dieses Subnetz wird während der IPCP Verhandlung bezogen.

Subnet Maske:

Stellt die Subnetz Maske, die für das lokale IP Interface zum PPP Transport verwendet wird zur Verfügung. Wenn die Angabe 0.0.0.0 ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet.

Route Maske:

Stellt die Subnetz Maske, die für die Route benutzt wird, wenn ein PPP Link aufkommt, zur Verfügung. Wenn die Angabe 0.0.0.0 ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet.

MRU:

Maximum Receive Unit. Dies wird vereinbart während der LCP Protokoll Phase.

Finde Primären / Sekundären DNS:

Diese Einstellung aktiviert / deaktiviert ob die primäre/sekundäre DNS Server Adresse vom Remote PPP Peer über IPCP angefragt wird. Die Standardeinstellung hierbei ist „wahr".

Übergebe DNS an Relay:

Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen Remonte Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an das lokale DNS Relay weitergeben so das die Verbindung aufgebaut werden kann.

Übergebe DNS an Client:

Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen Remonte Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an die lokalen Clients weitergeben so das die Verbindung aufgebaut werden kann.

Übergebe DNS an DHCP Server:

Ähnlich wie oben, aber gibt die DNS Server Adresse an den DHCP Server weiter.
Finde Primären NBNS / Sekundären NBNS: Diese Einstellung aktiviert / deaktiviert ob die primäre / sekundäre NBNS Server Adresse vom Remote Peer über IPCP angefragt wird. Der Standardwert dafür ist „falsch".

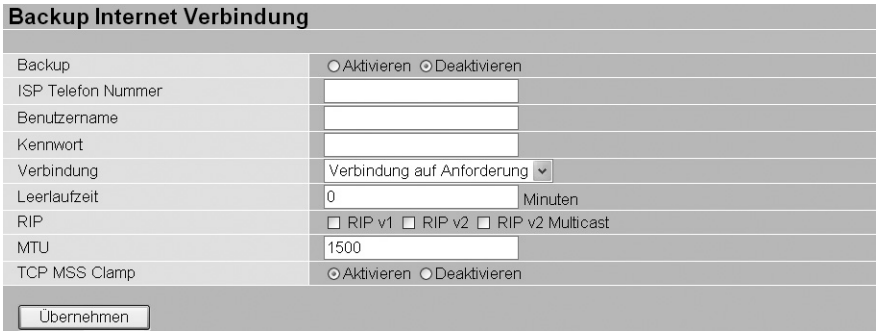
Finde Subnet Maske:

Gibt an, ob die Subnetzmaske während der IPCP Verhandlung benutzt wird oder nicht.

Übergebe Subnet Maske an DHCP Server:

Aktiviert um Ihre DHCP Server Einstellungen zu verändern mit den Informationen die Sie während des IPCP Verhandlung erhalten.

Backup ISP



Backup:

Wenn die Funktion aktiviert ist, wird der Router über ISDN eine Internetverbindung aufbauen sofern die Verbindung über ADSL nicht möglich ist.

ISP Telefon Nummer:

Geben Sie die Internet-Einwahl-Nummer Ihres ISP an.

Benutzername:

Geben Sie Ihren Benutzernamen ein, den Sie von Ihrem Provider erhalten haben. Sie können bis zu 128 alphanumerische Zeichen eingeben (Gross- und Kleinschreibung beachten). Sehr oft in der Form „benutzername@ispname“ anstelle “Benutzername”.

Für T-Online setzt sich der Benutzername aus Anschlusskennung T-OnlineNummer#Mitbenutzer zusammen, z. B. 123456789012123456789012#0001)

Passwort:

Geben Sie das zu dem Benutzernamen gehörende Passwort ein. Sie können bis zu 128 alphanumerische Zeichen eingeben (Gross- und Kleinschreibung beachten).

Verbindung:

- Ständig verbunden: Wenn Sie möchten, das der Router eine PPP Sitzung startet sobald er an ist und diese nach

Verbindungsabbruch durch den ISP automatisch wieder aufbaut (z.B. Zwangstrennung).

- Verbindung auf Anforderung: Wenn Sie eine PPP Sitzung nur dann möchten, wenn ein Paket Zugang zum Internet verlangt (z.B.: wenn ein Programm auf Ihrem Computer Zugriff zum Internet verlangt).

Wir empfehlen die Option Ständig verbunden nur dann zu aktivieren, wenn Sie über eine ISDN-Flatrate verfügen. Ansonsten können sehr hohe Kosten anfallen.

Leerlaufzeit:

Automatischer Verbindungsabbau des Router wenn keine Aktivität für eine voreingestellte Zeit stattfindet.

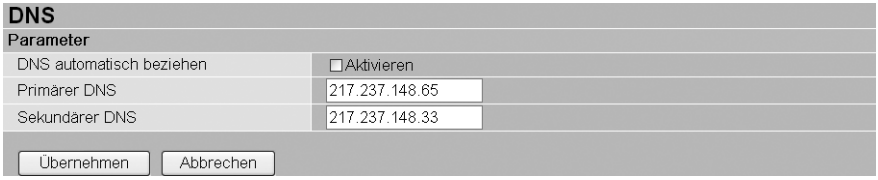
RIP:

RIP v1, RIP v2, und RIP v2 Multicast. Wählen Sie dies aus, um die RIP Funktion zu aktivieren.

MTU:

Maximum Transmission Unit. Die Größe des größten Datagramm (ohne media-spezifische Header) welche IP durch das Interface hindurchsenden wird.

DNS



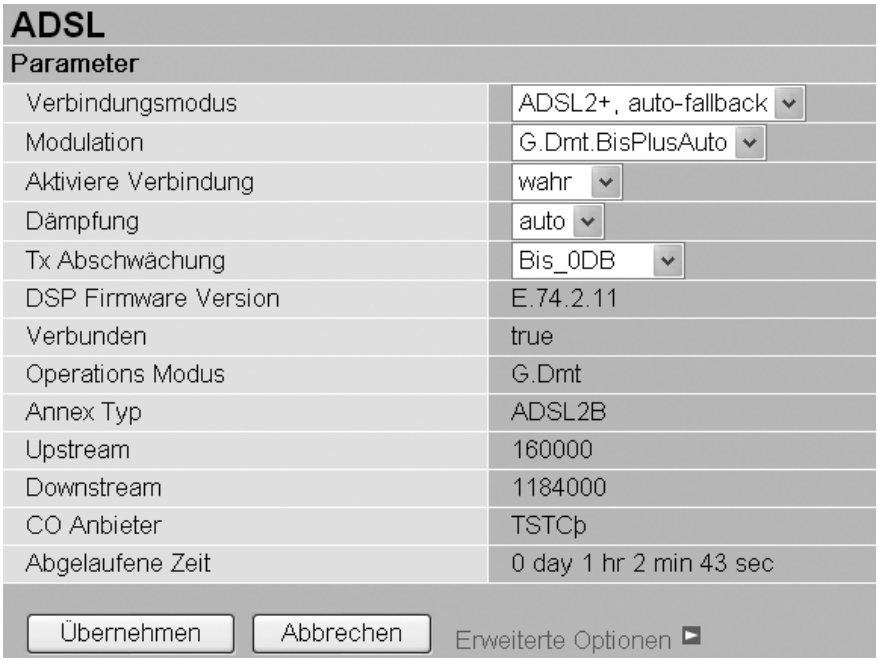
Das Domain-Name-System (DNS) beinhaltet ein Verzeichnis für Domain-Namen und deren IP-Adressen. Im Internet hat jeder Host einen Namen, z.B. www.google.de, den man sich meist gut merken kann und eine IP-Adresse. Da man sich die IP-Adresse hingegen schlecht merken kann, reicht es, den Domain-Namen einzugeben, der vom DNS in die entsprechende IP-Adresse konvertiert wird. Eine IP Adresse ist eine 32-Bit Nummer in der Form xxx.xxx.xxx.xxx, zum Beispiel 192.168.2.1. Sie können Sich eine IP Adresse wie eine Telefonnummer für ein Gerät im Internet vorstellen und der DNS erlaubt es

Ihnen die Telefonnummer für jeden speziellen Namen zu finden. Weil man sich eine IP Adresse schwer merken kann, konvertiert das DNS diese in einen Benutzerfreundlichen Namen mit Ihrer dazugehörigen IP Adresse.
Sie können die Domain Name System (DNS) IP Adresse automatisch von Ihrem ISP bekommen, wenn er dies beim Login anbietet. Normalerweise wenn Sie PPPoE oder PPPoA als Ihr WAN – ISP Protokoll wählen, wird Ihr ISP Ihnen die notwendigen DNS IP Adressen automatisch übermitteln. Sie können das Konfigurationsfeld leer lassen.

Alternativ kann Ihr ISP Ihnen die IP Adressen seines DNS mitteilen. In diesem Falle geben Sie die DNS IP Adressen hier ein.

Wenn Sie ein anderes der drei weiteren Protokolle auswählen — RFC1483m, Routed/Bridged und IPoA prüfen Sie bitte bei Ihrem ISP, ob Sie die IP Adressen für deren DNS Server erhalten. Diese DNS Server IP Adressen müssen Sie eingeben, wenn Sie die DNS Ihres PC auf die LAN IP des Routers einstellen.

ADSL



Verbindungsmodus:

Die Standardeinstellung ist Multimode. Dieser Modus wird automatisch den ADSL Line Code erkennen (G.dmt, G.lite, und T1.413). In manchen Gegenden kann es den ADSL Verbindungsmodus nicht erkennen. Stellen Sie hierfür den ADSL Verbindungsmodus zuerst auf T1.413 oder G.dmt. Falls es weiterhin fehlschlägt, versuchen Sie andere Einstellungen wie ALCTL, ADI, etc.

Aktiviere Verbindung:

Unterbrechen (falsch) Ihrer ADSL Leitung und Aktivierung (wahr) Ihrer ADSL Leitung wenn Sie den Verbindungsmodus verändert haben.

Coding Gain:

Konfiguriert den ADSL Coding Gain von 0 dB bis 7dB, oder automatisch.

Tx Abschwächung:

Stellt den ADSL transmission gain ein, der Wert ist zwischen 0 - 12.

DSP Firmware Version:

Aktuelle ADSL Line Code Firmware Version.

Verbunden:

Zeigt den aktuellen ADSL Leitungs-SYNC Status an.

Operations Modus:

Zeigt den aktuellen ADSL Modus Standard (Verbindungsmodus) Ihres Routers an sobald die ADSL Leitung synchronisiert ist.

Annex Typ:

ADSL Annex A, welches über einen normalen Telefonanschluss arbeitet. Annex B welches über eine ISDN Leitung arbeitet.

Upstream:

Zeigt die aktuelle Upstream Rate Ihrer ADSL Leitung an.

Downstream:

Zeigt die aktuelle Downstream Rate Ihrer ADSL Leitung an.

Erweiterte Optionen

ADSL

Parameter

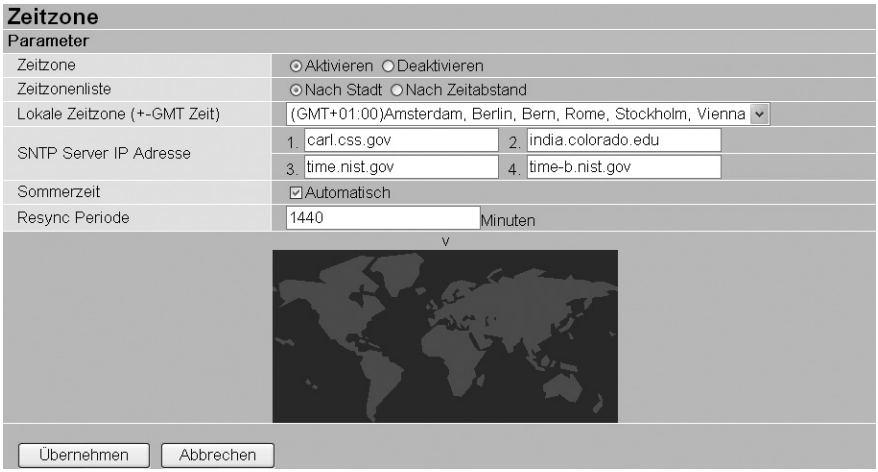
	Downstream	Upstream
SNR Bandbreite	30.5 dB	27 dB
Leitungsdämpfung	31.0 dB	19.5 dB
CRC Fehler	2	0
Latenz	Interleave	Interleave

Aktualisieren Zurück

System

Es gibt sechs Unterpunkte im Menü System: **Zeitzone, Remote Zugriff, Firmware Upgrade, Sichern/Wiederherstellen, Neustart** und **Benutzer Verwaltung.**

Zeitzone



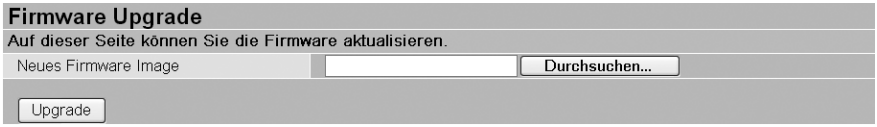
Der Router verfügt nicht über eine Echtzeit-Uhr, sondern über das Simple Network Time Protocol (SNTP), um über den SNTP Server im äußeren Netzwerk die richtige Uhrzeit vermittelt zu bekommen. Bitte wählen Sie die entsprechende Zeitzone und klicken dann auf „Übernehmen“. Sie erhalten die korrekte Zeitangabe, wenn Sie mit dem Internet verbunden sind. Die Uhrzeit wird im Status-System-Fenster angezeigt. Wenn Sie es vorziehen, Ihren eigenen SNTP Server einzurichten, geben Sie diesen bitte ein und wählen ihn aus. Ihr ISP bietet möglicherweise auch einen SNTP Server zur Benutzung an.
Sommerzeit: Viele Orte auf der Welt stellen die Zeit um, damit eine Stunde des Tageslichtes vom morgen auf den Abend verschoben wird. Aktivieren Sie das Kontrollkästchen damit dies automatisch umgestellt wird.
Resync Periode (in Minuten) ist das periodische Intervall in der der Router die Zeit erneut mit dem SNTP Server synchronisiert. Um einen erhöhten Verkehr zu Ihrem SNTP Server zu vermeiden, sollten Sie das Intervall so hoch wie möglich einstellen – zumindest alle paar Stunden oder sogar mehrere Tage.

Remote Zugriff

Um vorläufigen Fernzugriff auf den Router zu ermöglichen (z.B. außerhalb des LAN) wählen Sie die Zeitspanne wo Fernzugriffe erlaubt sind und klicken Sie auf Aktiviert. Sie können auch andere Konfigurationsoptionen für die Web Administration im Abschnitt Geräte Management im Menüpunkt Erweitert im GUI festlegen.

Wenn Sie den Fernzugriff permanent ermöglichen wollen, so geben Sie bitte 0 Minuten ein.

Firmware Upgrade



Die Firmware des Routers ist eine Software die alle Funktionen ermöglicht. Stellen Sie sich den Router als einen Computer vor und die Firmware ist die Software womit der Router arbeitet. Nach einiger Zeit wird möglicherweise die Software für den Router verbessert und modifiziert und er kann aktualisiert werden um diese Neuheiten und Vorzüge zu nutzen.

Sie finden dann diese neue Firmware im Internet. Unter http://www.t-com.de finden Sie auf der Startseite einen Link zu Faq & Downloads. Dort unter Software und Treiber den Link zu Downloads. Wählen Sie Speedport 400P.
Speichern Sie die neue Firmware auf Ihrem Rechner.
Klicken Sie auf Durchsuchen und Sie können die neue Firmware Version

auswählen, welche Sie sich heruntergeladen haben. Klicken Sie auf „Upgrade“ um die Firmware des Routers zu aktualisieren.

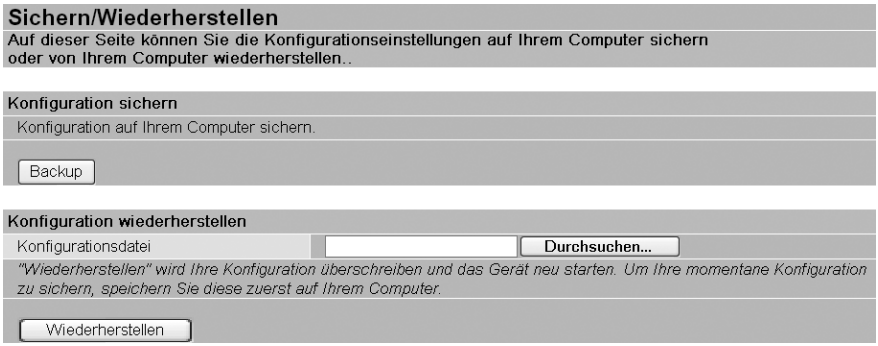
!

Schalten Sie Ihren Router NICHT aus oder unterbrechen den Firmware Upgrade Prozess. Dies kann den Router beschädigen.

Tipp

Informieren Sie sich bitte in regelmäßigen Abständen auf der Internetseite www.t-com.de über Neuerungen und Software-Updates.

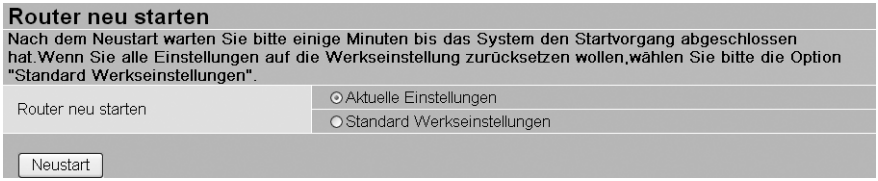
Sichern / Wiederherstellen


Sichern/Wiederherstellen
Auf dieser Seite können Sie die Konfigurationseinstellungen auf Ihrem Computer sichern oder von Ihrem Computer wiederherstellen..
Konfiguration sichern
Konfiguration auf Ihrem Computer sichern.
Backup
Konfiguration wiederherstellen
Konfigurationsdatei
Durchsuchen...
"Wiederherstellen" wird Ihre Konfiguration überschreiben und das Gerät neu starten. Um Ihre momentane Konfiguration zu sichern, speichern Sie diese zuerst auf Ihrem Computer.
Wiederherstellen

Diese Funktion erlaubt es Ihnen die aktuellen Einstellungen des Router zu sichern oder ein gesichertes File wiederherzustellen. Dies ist sehr nützlich, wenn Sie mit verschiedenen Einstellungen arbeiten oder experimentieren wollen. Wir empfehlen, die Einstellungen zu sichern, bevor Sie irgendwelche signifikanten Veränderungen an den Einstellungen des Routers vornehmen wollen.
Klicken Sie auf Sicherung um auszuwählen, wohin Sie das File auf Ihrem PC abspeichern wollen. Sie können auch den Filenamen ändern, wenn Sie mehrere Backups haben wollen.
Klicken Sie auf Durchsuchen um ein File auszuwählen, welches Sie von Ihrem PC wiederherstellen möchten. Verwenden Sie nur Backup Files die von der Backupfunktion des Routers selber erzeugt worden sind und die von der gleichen Firmware Version des Router sind. Editieren Sie auf keinen Fall das File auf Ihrem PC manuell.
Nachdem Sie das File ausgewählt haben, was Sie wiederherstellen wollen, klicken Sie auf Wiederherstellen um das File in den Router zu laden.

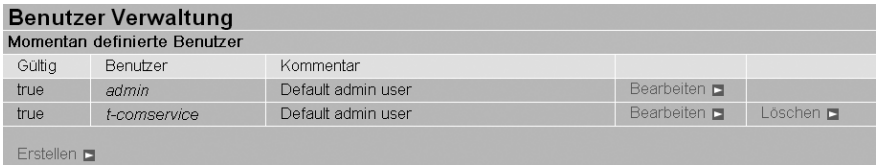
Neustart

Klicken Sie auf Neustart mit der Option Aktuelle Einstellungen um den Router neu zu starten (und um die letzte im Router gespeicherte Einstellung wiederherzustellen).

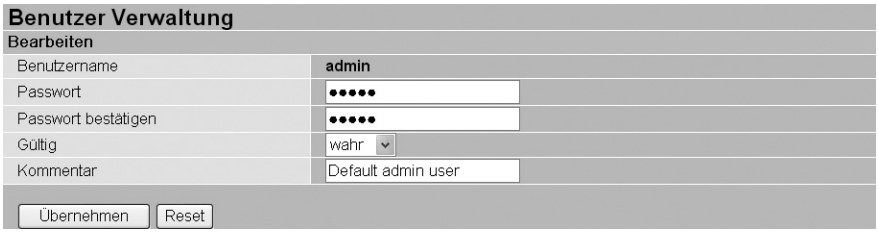

Router neu starten
Nach dem Neustart warten Sie bitte einige Minuten bis das System den Startvorgang abgeschlossen hat.Wenn Sie alle Einstellungen auf die Werkseinstellung zurücksetzen wollen,wählen Sie bitte die Option "Standard Werkseinstellungen".
Router neu starten
Aktuelle Einstellungen
Standard Werkseinstellungen
Neustart

Wenn Sie den Router mit den Werkseinstellungen neu starten wollen (z.B. nach einem Firmware Upgrade oder einer defekten Konfiguration) so klicken Sie die Standard Werkseinstellungen Box an.
Sie können auch einen Reset auf die Werkeinstellungen durchführen, indem Sie den kleinen Resetschalter auf der Rückseite des Routers länger als 6 Sekunden drücken wenn der Router eingeschaltet ist.

Benutzer Verwaltung



Damit sichergestellt werden kann, dass nur authorisierte Benutzer zugriff auf den Router erhalten, müssen alle Benutzer sich mit einem Passwort einloggen.
Sie können vorhandene Benutzer bearbeiten und neue Benutzer erstellen welche die Zugriffsberechtigung auf den Router erhalten. Wenn Sie auf Bearbeiten klicken erhalten Sie folgende Optionen:

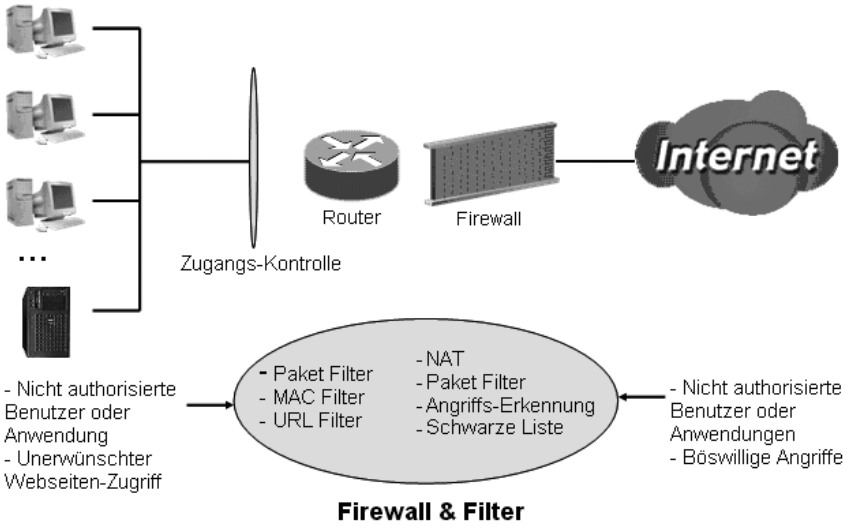


Sie können dann das Passwort des Nutzers verändern, welcher aktiv und Gültig ist, als auch einen Kommentar zu jedem Benutzer hinzufügen. Diese Optionen sind die selben wenn Sie einen Benutzer neu anlegen, mit der Ausnahme das Sie den Benutzernamen nicht ändern können. Sie können den Standardmäßigen Admin Benutzer nicht löschen, aber jeden anderen Benutzer indem Sie auf Löschen klicken.

Wir empfehlen Ihnen das Standardpasswort des Admin Benutzer zu ändern, nachdem Sie den Router angeschlossen haben und jederzeit, wenn Sie einen Reset auf die Werkeinstellungen durchgeführt haben. Standardmäßig ist das Passwort “admin“.

Firewall und Zugangskontrolle

Ihr Router hat eine SPI (Stateful Packet Inspection) Firewall um den Internetzugang von Ihrem LAN zu kontrollieren und um Hackerattacken zu verhindern. Zusätzlichen wenn Sie NAT nutzen (Network Address Translation; schauen Sie im Abschnitt WAN Konfiguration für weitere Details nach), fungiert der Router als eine Art „natürliche“ Firewall, weil alle Ihre PCs im LAN private IP Adressen nutzen, die nicht direkt aus dem Internet angesprochen werden können.



Firewall:

Unterbindet Zugang von außerhalb auf Ihr Netzwerk. Der Router bietet 3 Sicherheitsstufen an.

NAT natural Firewall:

Diese maskiert die LAN Nutzer IP Adressen, die nach außen hin unsichtbar sind und es ist sehr viel schwieriger für einen Hacker ein Ziel in Ihrem Netzwerk auszumachen. Diese natürliche Firewall ist aktiv, sobald Sie NAT aktiviert haben.

Wenn Sie Virtuelle Server für Ihren PC nutzen, wird Ihr PC entsprechend geöffnet bis zu dem Grad, den Sie in den Virtuellen Server Einstellungen vorgenommen haben. Diese Ports müssen in der Firewall als Paket Filter ebenfalls geöffnet sein.

Firewall Security und Policy (Generelle Einstellungen):
Ankommende Richtung der Paket Filter Regeln verhindern unerlaubten Computern oder Programmen Zugriff auf das Lokale Netzwerk vom Internet aus.

Angriffserkennung:
Aktiviere Angriffserkennung um boshafte Angriffe zu bemerken, verhindern und loggen.

Zugangskontrolle:
Verhindert Zugang von Ihren PCs im lokalen Netzwerk.

Firewall Security und Policy (Generelle Einstellungen):
Ausgehende Richtung von Paket Filter Regeln um unerlaubten Zugriff von Computern oder Programmen zu verhindern.

URL Filter:
Um bestimmte Webseiten zu blockieren, die vom Lokalen Netzwerk besucht werden wollen.

Es gibt fünf Unterpunkte im Menü Firewall: **Generelle Einstellungen, Paket Filter, Angriffserkennung, URL Filter** und **Firewall Protokoll.**

Generelle Einstellungen

Sie können die Firewall deaktivieren, alle Filterregeln selber einstellen oder die Firewall aktivieren und damit die voreingestellten Regeln nutzen, diese aber selber noch modifizieren so wie Sie es wünschen. Der Paket Filter kann verwendet werden um Port basierte Anwendungen und IP Adressen zu filtern.

Es gibt vier Optionen wenn Sie die Firewall aktivieren, diese sind:

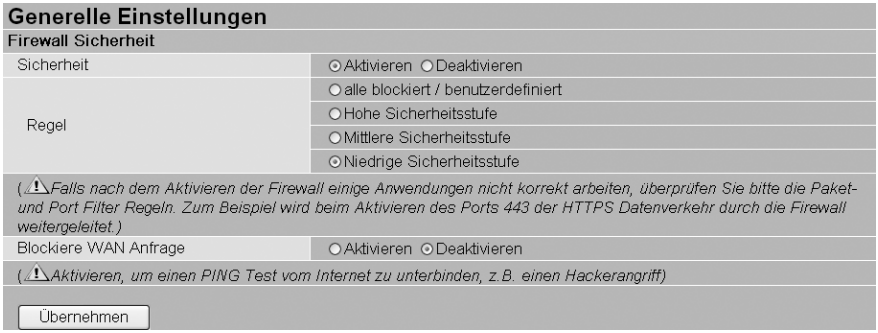
- Alle blockiert/Benutzerdefiniert: keine vordefinierten Port- oder Adressregeln. Jedes hereinkommende (Internet nach LAN) und herausgehende (LAN nach Internet) Paket wird blockiert. Benutzer müssen Ihre eigenen Filterregeln aufstellen, um ins Internet gehen zu können.

- Hohe/Mittlere/Niedrige Sicherheitsstufe: Die vordefinierten Paket Filter Regeln für Hohe, Mittlere und Niedrige Sicherheitsstufe werden als Paket Filter Regeln im Menüabschnitt Paket Filter angezeigt.

Wählen Sie entweder Hohe, Mittlere oder Niedrige Sicherheitsstufe um die Firewall zu aktivieren. Der einzige Unterschied zwischen diesen 3 Sicherheitsstufen, ist die Voreinstellungen der Paket Filter Regeln im Abschnitt Paket Filter. Die Firewall Funktionalität ist die gleiche für alle Einstellungen; es ist nur die Liste der voreingestellten Paket Filter die sich dabei ändert.

Wenn Sie die voreingestellten Sicherheitsstufen wählen und dann eigene Filter hinzufügen, können Sie vorläufig die Firewall deaktivieren und Ihre eigenen Einstellungen wiederherstellen wenn Sie den gleichen Sicherheitslevel wählen.

“Blockiere WAN Anfrage” ist eine eigene Funktion und steht nicht im Zusammenhang ob die Sicherheit aktiviert oder deaktiviert ist. Hauptsächlich ist es um einen Scan von einer WAN Seite durch Hacker zu unterbinden.


Generelle Einstellungen
Firewall Sicherheit
Sicherheit
Aktivieren
Deaktivieren
Regel
alle blockiert / benutzerdefiniert
Hohe Sicherheitsstufe
Mittlere Sicherheitsstufe
Niedrige Sicherheitsstufe
(Falls nach dem Aktivieren der Firewall einige Anwendungen nicht korrekt arbeiten, überprüfen Sie bitte die Paket- und Port Filter Regeln. Zum Beispiel wird beim Aktivieren des Ports 443 der HTTPS Datenverkehr durch die Firewall weitergeleitet.)
Blockiere WAN Anfrage
Aktivieren
Deaktivieren
(Aktivieren, um einen PING Test vom Internet zu unterbinden, z.B. einen Hackerangriff)
Übernehmen

Vorsicht! Diese Einstellungen sollten Sie nur vornehmen, wenn Sie sich sicher sind, was die Einstellungen bewirken. Infolge dieser Einstellungen kann die Schutzfunktion der Firewall vollständig oder teilweise ausgeschaltet werden. Dadurch könnte möglicherweise die Integrität Ihrer Daten gefährdet werden oder unberechtigten Personen könnten möglicherweise unbemerkt Zugang zu Ihren Daten erhalten. Im Auslieferzustand ist die Firewall aktiviert (Niedrige Sicherheitsstufe).

Jeder Remote Benutzer der versucht obige Einstellung vorzunehmen, kann eine Blockade der Konfiguration und des Router Management vom Internet aus hervorrufen. Daher nehmen Sie diese Einstellungen bitte vom LAN vor.

Paket Filter

Diese Funktion steht nur zur Verfügung wenn die Firewall aktiviert ist und eine der vier Sicherheitsstufen ausgewählt wurde (Alle blockiert, Hohe, Mittlere und Niedrige Sicherheitsstufe). Die vordefinierten Paket Filter Regeln in der Paket Filter Liste sind der Sicherheitsstufe angepasst. Siehe Tabelle 1: Voreingestellte Paket Filter Regeln für weitere Informationen.

Paket Filter

TCP/UDP Filter hinzufügen ▶ | Raw IP Filter hinzufügen ▶

Paket Filter Regeln

Regel-Name	Zeitplan	Quell IP / Netzmaske Ziel IP / Netzmaske	Protokoll	Quell Port(s) Ziel Port(s)	Eingehend Ausgehend		
mei_http	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_dns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_tdns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_ftp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_tnet	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_smtp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_pop3	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_nntp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 119 ~ 119	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_rav	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 7070 ~ 7070	Erlauben Erlauben	Bearbeiten ▶	Löschen ▶
mei_icmp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	ICMP	N/A N/A	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶

Beispiel: Voreingestellte Paket Filter Regeln

Die vordefinierten Paket Regeln für Hohe, Mittlere und niedrige Sicherheitsstufen lauten wie folgt.

Hinweis: Firewall – Alle Blockiert/Benutzerdefiniert, Sie müssen die Port Filter Regeln selber definieren. Es gibt keine Voreinstellung.

Tabelle 1: Voreingestellte Paket Filter									
Anwendung	Protokoll	Port Nummer		Firewall - Hohe		Firewall - Mittlere		Firewall – Niedrige	
		Start	End	Eingehend	Ausgehend	Eingehend	Ausgehend	Eingehend	Ausgehend
HTTP(80)	TCP(6)	80	80	NEIN	JA	NEIN	JA	NEIN	JA
DNS (53)	UDP(17)	53	53	NEIN	JA	NEIN	JA	JA	JA
DNS (53)	TCP(6)	53	53	NEIN	JA	NEIN	JA	JA	JA
FTP(21)	TCP(6)	21	21	NEIN	NEIN	NEIN	JA	NEIN	JA
Telnet(23)	TCP(6)	23	23	NEIN	NEIN	NEIN	JA	NEIN	JA
SMTP(25)	TCP(6)	25	25	NEIN	JA	NEIN	JA	NEIN	JA
POP3(110)	TCP(6)	110	110	NEIN	JA	NEIN	JA	NEIN	JA
NEWS(119) (Network News Transfer Protocol)	TCP(6)	119	119	NEIN	NEIN	NEIN	JA	NEIN	JA
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	NEIN	NEIN	JA	JA	JA	JA
PING	ICMP(1)	N/A	N/A	NEIN	JA	NEIN	JA	NEIN	JA
H.323(1720)	TCP(6)	1720	1720	NEIN	NEIN	NEIN	JA	JA	JA
T.120(1503)	TCP(6)	1503	1503	NEIN	NEIN	NEIN	JA	JA	JA
SSH(22)	TCP(6)	22	22	NEIN	NEIN	NEIN	JA	JA	JA
NTP(123)	UDP(17)	123	123	NEIN	JA	NEIN	JA	NEIN	JA
HTTPS(443)	TCP(6)	443	443	NEIN	NEIN	NEIN	JA	NEIN	JA
ICQ (5190)	TCP(6)	5190	5190	NEIN	NEIN	NEIN	NEIN	JA	JA
SIP REG	UDP(17)	5060	5070	NEIN	NEIN	NEIN	NEIN	JA	JA
SIP RTP	UDP(17)	30000	30005	NEIN	NEIN	NEIN	NEIN	JA	JA
SIP STUN	UDP(17)	3478	3479	NEIN	NEIN	NEIN	NEIN	JA	JA
IKE	UDP(17)	500	500	NEIN	NEIN	NEIN	NEIN	JA	JA
L2TP	UDP(17)	1701	1701	NEIN	NEIN	NEIN	NEIN	JA	JA
PPTP	TCP(6)	1723	1723	NEIN	NEIN	NEIN	NEIN	JA	JA
GRE	GRE(47)	N/A	N/A	NEIN	NEIN	NEIN	NEIN	JA	JA
IPSec	UDP(17)	4500	4500	NEIN	NEIN	NEIN	NEIN	JA	JA

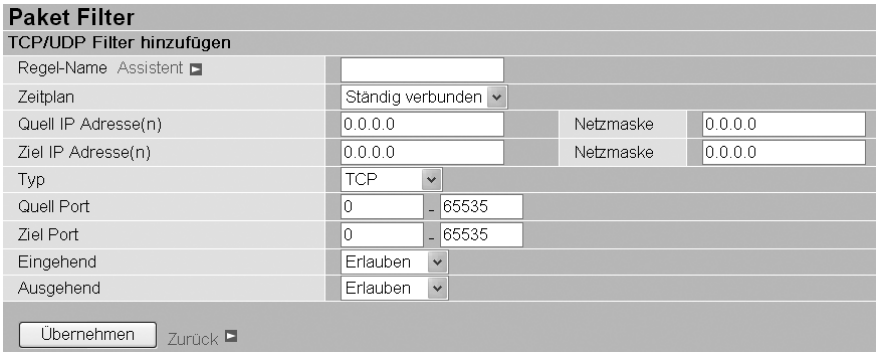
Eingehend:

Internet zum LAN

Ausgehend:

LAN zum Internet.

Paket Filter –TCP/UDP Filter hinzufügen



Regelname:

Beschreibung der Regel durch den Benutzer.

Zeitplan:

Sie können den Zeitplan selber definieren. So können Sie bestimmte Regeln zu bestimmten Tageszeiten aktivieren. Für weitere Informationen hierfür lesen Sie bitte das Kapitel Zeitplan.

Quell IP Adress(n) / Ziel IP Adress(n):

Dies ist der IP Adressen Filter, mit welchem Sie Datenverkehr von/zu bestimmten IP-Adressen erlauben/blockieren. Tragen Sie ebenfalls die Subnet Maske des IP Adressen Bereiches ein. Tragen Sie bei den IP Adressen und der Subnet Maske 0.0.0.0 wird der IP Adressen Filter nicht angewandt bzw. gilt für alle Adressen.

Tipp

Um einen Zugang zu blockieren von/zu einer einzigen IP Adresse, tragen Sie die gewünschte IP Adresse ein und geben als Subnet Maske “255.255.255.255” an.

Typ:

Ist der Paket Protokoll Typ. Wählen Sie TCP, UDP oder beide TCP/UDP.

Quell Port:

Dieser Port oder der Port Bereich definiert den Port welcher von Remote/WAN (Internet) die Verbindung zur der lokalen Anwendung erhält oder nicht. Die Werkseinstellung lautet 0 ~ 65535. Es wird

empfohlen dass diese Option von einem erfahren Anwender vorgenommen wird.

Ziel Port:

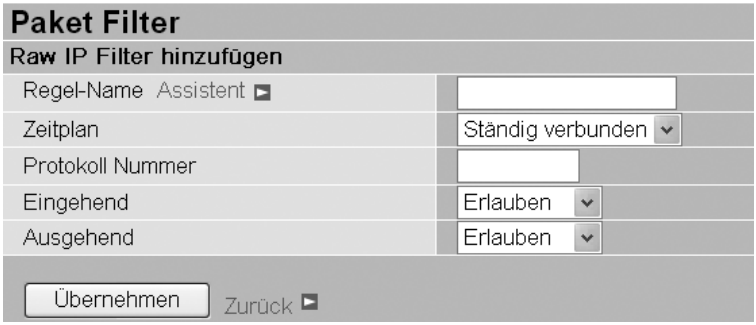
Dieser Port oder der Port Bereich definiert die Anwendung.

Eingehend / Ausgehend:

Wählen Sie Erlauben/Blockieren für den Zugriff zum Internet (Ausgehend) oder vom Internet (Eingehend).

Klicken Sie auf **Übernehmen** damit die Einstellungen übernommen werden.

Paket Filter – Raw IP Filter hinzufügen



Regelname:

Beschreibung der Regel durch den Benutzer.

Zeitplan:

Sie können den Zeitplan selber definieren. So können Sie bestimmte Regeln zu bestimmten Tageszeiten aktivieren. Für weitere Informationen hierfür lesen Sie bitte das Kapitel Zeitplan.

Protokoll Nummer:

Tragen Sie die Port Nummer ein, z.B. GRE 47.

Eingehend / Ausgehend:

Wählen Sie Erlauben/Blockieren für den Zugriff zum Internet (Ausgehend) oder vom Internet (Eingehend).

Klicken Sie auf **Übernehmen** damit die Einstellungen übernommen werden.

Beispiel:
Konfiguration der Firewall für einen Zugriff vom Internet auf den Webserver des Router

Die voreingestellte Paket Filter Regel für HTTP (TCP Port 80) ist jeweils die gleiche, egal ob die Sicherheitsstufe auf Hohe, Mittlerer oder Niedrige Sicherheitsstufe eingestellt ist. Wenn Sie vom Internet auf den Webserver des Routers in Ihrem lokalen Netzwerk (LAN) zugreifen wollen und die Firewall aktiviert ist, müssen Sie die Paket Filter Regel für HTTP bearbeiten.

Wie Sie unten sehen können, sobald die Firewall aktiviert ist mit einer der drei Sicherheitsstufen (Hohe/Mittlere/Niedrige), ist der eingehende Zugang über HTTP nicht erlaubt.

Hinweis: Eingehend bedeutet vom Internet zum LAN, Ausgehend vom LAN zum Internet

Paket Filter

TCP/UDP Filter hinzufügen ▶ | Raw IP Filter hinzufügen ▶

Paket Filter Regeln

Regel-Name	Zeitplan	Quell IP / Netzmaske Ziel IP / Netzmaske	Protokoll	Quell Port(s) Ziel Port(s)	Eingehend Ausgehend		
mei_http	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_dns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_tdns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_ftp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_tnet	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_smtp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_pop3	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_nntp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 119 ~ 119	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_rav	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 7070 ~ 7070	Erlauben Erlauben	Bearbeiten ▶	Löschen ▶
mei_icmp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	ICMP	N/A N/A	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶

Konfiguration Paket Filter:

1. Klicken Sie auf Paket Filter. Sie sehen nun die Seite Paket Filter Regeln (in diesem Fall Niedrige Sicherheitsstufe):

Hinweis: Sie können auch auf **Bearbeiten** klicken, anstelle auf **Löschen**. Das Beispiel zeigt wie eine Paket Filter Regel hinzugefügt wird. Daher wird der vorhandene Eintrag zuerst gelöscht.

Paket Filter

TCP/UDP Filter hinzufügen ▶ | Raw IP Filter hinzufügen ▶

Paket Filter Regeln — **Klick Löschen**

Regel-Name	Zeitplan	Quell IP / Netzmaske Ziel IP / Netzmaske	Protokoll	Quell Port(s) Ziel Port(s)	Eingehend Ausgehend		
mei_http	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_dns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_tdns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_ftp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_tnet	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_smtp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_pop3	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_nntp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 119 ~ 119	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶
mei_rav	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 7070 ~ 7070	Erlauben Erlauben	Bearbeiten ▶	Löschen ▶
mei_icmp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	ICMP	N/A N/A	Blockieren Erlauben	Bearbeiten ▶	Löschen ▶

2. Klicken Sie auf Löschen damit die existierende Paket Filter Regel für HTTP entfernt wird.

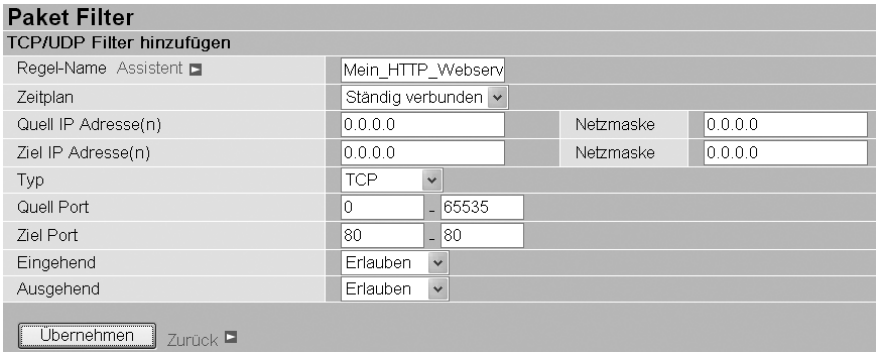
3. Klicken Sie auf TCP/UDP Filter hinzufügen.

Paket Filter — **Klick TCP/UDP Filter hinzufügen**

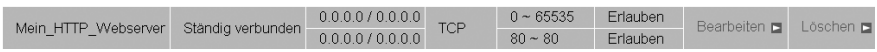
TCP/UDP Filter hinzufügen ▶ | Raw IP Filter hinzufügen ▶

4. Tragen Sie einen Regel Namen ein, Wählen Sie den Zeitplan, Quell und Ziel IP Adressen, Typ, Quell und Ziel Port, Eingehend und Ausgehend.

Beispiel:
Regel Name: Mein_HTTP_Webserver
Zeitplan: Always On
Quelle / Ziel IP Adresse(n): 0.0.0.0 **(Damit jeder vom Internet auf den Webserver des Router zugreifen kann, wird hier 0.0.0.0 eingetragen)**
Typ: TCP (Siehe auch Tabelle1: Voreingestellte Paket Filter)
Quell Port: 0-65535 **(Jeder Port erhält die Erlaubnis sich zu verbinden)**
Ziel Port: 80-80 **(Dieser Port definiert HTTP)**
Eingehend / Ausgehend: Erlauben

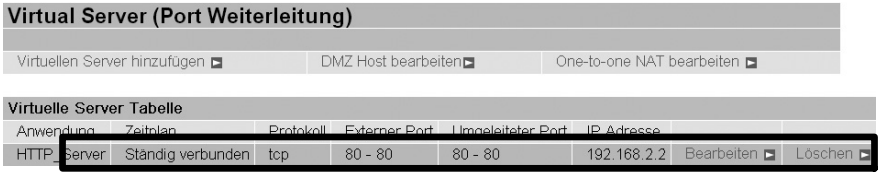


5. Die neue Paket Filter Regel sieht wie folgt aus:



6. Die Konfiguration des Virtuellen Servers (port forwarding/Portweiterleitung) muss nun vorgenommen werden, damit die HTTP Anfragen auf Port 80 zu dem lokalen Router weitergeleitet werden.

Hinweis: Wie Sie die Portweiterleitung für HTTP vornehmen, entnehmen Sie bitte dem Kapitel Virtuelle Server, Virtuelle Server hinzufügen.



Angriffserkennung

Die Angriffserkennung (Intrusion Detection System / IDS) des Routers wird benutzt, um Hacker Attacken und ein Eindringen aus dem Internet zu verhindern. Wenn die Angriffserkennung Funktion der Firewall aktiviert ist, werden hereinkommende Pakete gefiltert und blockiert, je nachdem ob Sie als eine mögliche Hackerattacke, Eindringversuch oder andere Verbindungen gilt, die dem Router verdächtig vorkommt.

Schwarze Liste:

Wenn der Router eine mögliche Attacke erkennt, wird die Verursacher IP oder Ziel IP in die Schwarze Liste (Blacklist) eingetragen. Jeder weitere Versuch diese IP zu nutzen wird so lange blockiert, wie die Zeiteinstellung in der Blockierungsdauer. Die Standardeinstellung dieser Funktion ist deaktiviert. Einige Angriffstypen werden direkt abgeblockt ohne die Schwarze Liste Funktionen zu nutzen, wie z.B. Land attack und Echo/CharGen Scan.

Angriffserkennung:

Wenn aktiviert, IDS blockiert Smurf Attacken. Werkseinstellung ist deaktiviert.

Blockierungsdauer:

- Angriffszielschutzdauer: Die Dauer für die Blockierung von Smurf attacks. Standardwert ist 600 Sekunden.

- Scanangriff Blockierungsdauer: Dies ist die Dauer für den Host der einen möglichen Scan Angriff gestartet haben. Scan Angriffstypen einschließlich X'mas scan, IMAP SYN/FIN scan und andere. Standardwert ist 86400 Sekunden.

- DoS Angriff Blockierungs-Zeitraum: Dies ist die Dauer des Blockens eines Hosts der einen möglichen Denial of Service (DoS) Angriff unternommen hat, inklusive Ascend Kill und WinNuke. Standardwert ist 1800 Sekunden.

Maximale Anzahl von TCP Open Handshakes:

Dies ist ein Schwellwert, der entscheidet, ob ein SYN Flood Angriff stattfindet oder nicht. Standardwert ist 100 TCP SYN per second.

Maximale PING Anzahl:

Dies ist ein Schwellwert, der entscheidet, ob ein ICMP Echo Storm stattfindet oder nicht. Standardwert ist 15 ICMP Echo Requests (PING) pro Sekunde.

Maximale ICMP Anzahl:

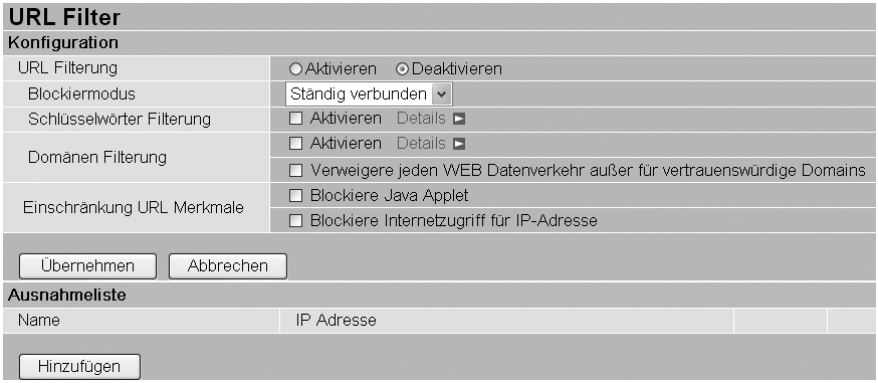
Dies ist ein Schwellwert, der entscheidet, ob ein ICMP flood stattfindet oder nicht. Standardwert ist 100 ICMP Packets pro Sekunde mit der Ausnahme von ICMP Echo Requests (PING). Für SYN Flood, ICMP Echo Storm und ICMP flood, warnt IDS den Benutzer im Event Log, es kann aber solche Attacken nicht verhindern.

Tabelle 2: Hacker Attack Typen welche von IDS erkannt werden					
Angriff Name	**Erkennungs Parameter**	**Schwarze Liste**	**Typen der Blockierungs Dauer**	**Paket verwerfen**	**Anzeige im Protokoll**
Ascend Kill	Ascend Kill data	Src IP	DoS	Ja	Ja
WinNuke	TCP Port 135, 137-139, Flag: URG	Src IP	DoS	Ja	Ja
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Ja	Ja
Land attack	SrcIP = DstIP			Ja	Ja
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Ja	Ja
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Ja	Ja
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Ja	Ja
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Ja	Ja
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Ja	Ja
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Ja	Ja
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Ja	Ja
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Ja	Ja
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Ja
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Ja
ICMP Echo	Max PING Count (Default 15 c/sec)				Ja

Src IP: Quell IP **Src Port:** Quell Port
Dst Port: Ziel Port **Dst IP:** Ziel IP

URL Filter

URL (Uniform Resource Locator – eine Adresse in der Form von **http://www.google.de/**) Filter Regeln erlauben es Benutzer aus dem Netzwerk bestimmte Internetseiten anzusteuern. Es gibt keine vordefinierten URL Filterregeln; Sie können diese Ihren Bedürfnissen anpassen.



Aktivieren/Deaktivieren:

URL Filter aktivieren bzw. deaktiveren.

Blockiermodus:

Auflistung der verschieden URL Filter Modis. Die Voreinstellung ist deaktiviert.

- Deaktiviert: Der URL Filter ist deaktiviert.
- Ständig verbunden: Der URL Filter ist aktiviert und überprüft permanent die Anfragen.
- TimeSlot1 bis TimeSlot16: Der von Ihnen gewählte Zeitplan. Sie können den URL Filter zu bestimmten Zeiten aktivieren, z.B. während den Bürozeiten. Für weitere Informationen hierfür lesen Sie bitte das Kapitel Zeitplan.

Schlüsselwörter Filterung:

Erlaubt es bestimmte Schlüsselwörter in einer URL zu blockieren anstelle einer kompletten URL. (z.B. ein Bild Namens “werbung.gif”). Wenn aktiviert, wird Ihre spezielle Schlüsselwörter Liste überprüft, ob ein Wort davon in der URL vorhanden ist und

dadurch blockiert wird. Bitte beachten Sie dass der URL Filter nur den Web Browser (HTTP) blockiert, die den Port 80 nutzen.

Zum Beispiel, die URL ist **http://www.google.de/abcde.html** und wird verworfen weil das Schlüsselwort “abcde” dort erscheint.

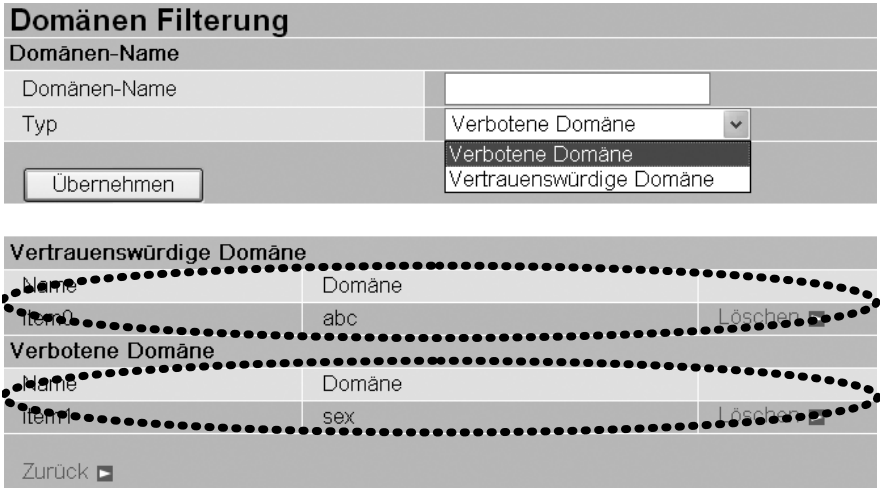
Diese Funktion überprüft, ob der Domain Name in der URL in der Liste der erlaubten oder verbotenen URLs ist. Wenn dies zutrifft, wird die URL Anforderung gesendet (Trust) oder verworfen (Forbidden). Für diese Funktion müssen beide Kontrollkästchen aktiviert sein. Die Prozedur ist wie folgt:

1. Prüft ob die Domain in der URL in der vertrauenswürdigen Liste ist. Wenn ja, wird die Verbindungsanfrage an den entfernten Server gesendet.

2. Wenn nicht, wird die verbotene Liste überprüft und die Verbindungsanfrage wird verworfen.

3. Wenn ein Paket keines der beiden Bedingungen erfüllt, wird die Anfrage an den entfernten Server gesendet.

4. Bitte beachten Sie das die Domain spezifiziert wird und nicht die volle URL. Zum Beispiel um Verkehr nach **www.sex.com**, geben Sie “sex” oder “sex.com” anstelle von **“www.sex.com“.** Im folgenden Beispiel wird die URL Anfrage für **www.abc.com** an den entfernten Server gesendet weil diese in den erlaubten Seiten enthalten ist während die URL Anfrage für www.sex oder **www.sex.com** nicht ausgeführt wird, weil sex.com in der verbotenen Liste enthalten ist.



Einschränkung URL Merkmale:

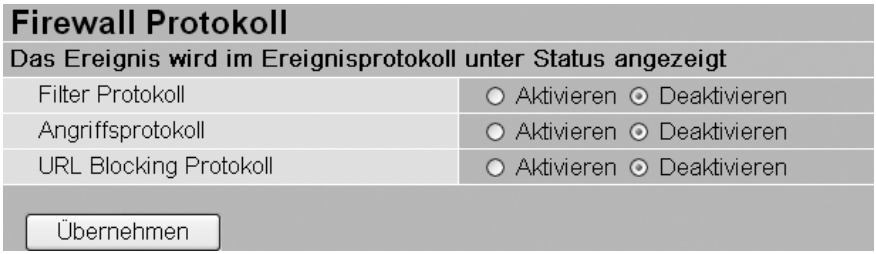
Diese Funktion erweitert die Einschränkung der URL Regeln.

Beispiel:

Andy möchte jeden WEB Datenverkehr deaktivieren, ausgenommen denen in der vertrauenswürdigen Domäne, damit verhindert wird das Bobby auf andere Webseiten zugreifen kann. Andy wählt beide Funktionen der Domänen Filterung und denkt Bobby hat nun keinen Zugriff auf andere Webseiten. Aber Bobby kennt die Funktion Domänen Filterung und weiss, dass er auf eine Webseite über deren IP Adresse zugreifen kann. Wenn dies der Fall ist, so ist die Funktion, Blockiere Internetzugriff für IP Adresse sehr hilfreich für Andy. Nun kann Andy verhindern dass Bobby Zugriff auf andere Seiten hat.

- Blockiere Java Applet: Diese Funktion kann Web Inhalte blockieren welche Java Applets beinhalten. Dies ist zum Schutz Ihres Systemes wenn jemand einen Angriff über ein HTTP Protokoll versucht.
- Blockiere Internetzugriff für IP Adresse: Verhindert das jemand die IP Adresse als URL benutzt um die Domain Filterung Funktion zu umgehen.

Firewall Protokoll



Das Firewall Protokoll zeigt die Informationen jeder unerwartenden Aktion Ihrer Firewall Einstellungen an.

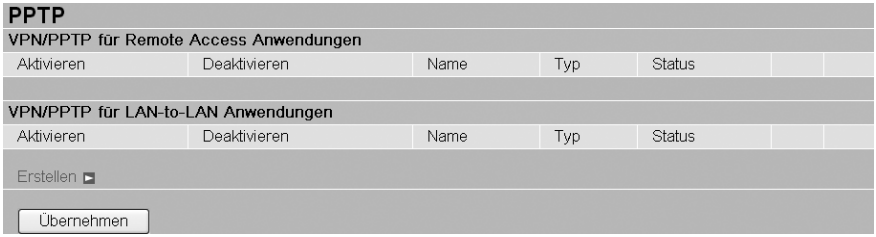
Klicken Sie auf Akitiveren damit diese Protokolle angezeigt werden.

Das Protokoll können Sie unter Status – Ereignis Protokoll einsehen nachdem es aktiviert wurde.

VPN (Virtual Private Networks)

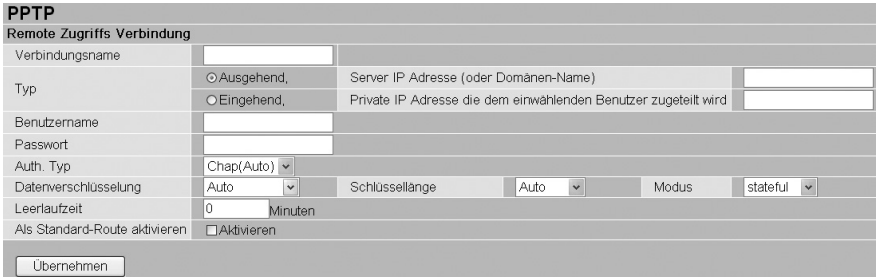
Ihr Router unterstützt drei Haupttypen von VPN (Virtual Private Network), **PPTP, IPSec** und **L2TP,** und diese finden Sie im Menü auf der linken Seite. Zusätzlich wird **ISDN Einwahl** unterstützt. Mit dieser Funktion haben Sie die Möglichkeit sich von außen per ISDN in Ihr Netzwerk einzuwählen.

PPTP



Es gibt zwei Typen von PPTP VPN die unterstützt werden. **Remote Access** und **LAN-to-LAN** (schauen Sie weiter unter für weitere Informationen.). Klicken Sie **Erstellen** um eine neue VPN Verbindung zu konfigurieren.

PPTP Remote Zugriffs Verbindung



Verbindungsname:

Dies erlaubt Ihnen die diese spezielle Verbindung zu identifizieren, z.B.: „Verbindung zum Büro“.

Typ:

Klicken Sie **Ausgehend** wenn Sie wollen das Ihr Router als Client

(verbindet zu einem entfernten VPN Server, z.B.: Ihr Büro Server), wählen Sie **Eingehend** arbeitet er als VPN Server.

- Wenn Sie den Router als Client konfigurieren, geben Sie die entfernte Server IP Adresse (oder Hostname) ein mit der Sie sich verbinden wollen.
- Wenn Sie den Router als Server konfigurieren, geben Sie die Private IP Adresse die dem einwählenden Benutzer zugeordnet wird ein.

Benutzername:

Wenn Sie ein „Ausgehender" Nutzer sind (client), geben Sie den Benutzernamen ein, der vom Host festgelegt wird. Wenn Sie ein „Eingehend" benutzter sind (server) geben Sie Ihren eigenen Benutzernamen ein.

Passwort:

Wenn Sie ein „Ausgehender" Nutzer sind (client), geben Sie das Passwort ein, das vom Host festgelegt wird. Wenn Sie ein „Eingehend" Benutzer sind (server), geben Sie Ihr eigenes Passwort ein.

Auth. Typ:

Standardwert ist **Auto,** wenn Sie wollen, das der Router den Authentication Typ selber erkennen soll oder aber wenn es CHAP (Challenge Handshake Authentication Protocol) oder PAP (Password Authentication Protocol) ist und Sie wissen welcher Typ vom Server benutzt wird. Wenn PAP benutzt wird, wird das Passwort unverschlüsselt gesendet, wobei CHAP das Passwort verschlüsselt, bevor es gesendet wird und auch es zu unterschiedlichen Momenten anfordert, um zu prüfen ob der Client nicht durch einen Eindringling ersetzt wurde.

Datenverschlüsselung:

Daten die über die VPN Verbindung gesendet werden, können mit einem MPPE Algorithmus verschlüsselt werden. Standardwert ist **Auto,** so das die Einstellung während des Verbindungsaufbaus ausgetauscht werden oder aber Sie können die Verschlüsselung auf **Aktiviert** oder **Deaktiviert** setzen.

Schlüssellänge:

Die Daten werden mit einem MPPE Algorithmus mit 40 Bit oder 128 Bit verschlüsselt. Standardwert ist **Auto,** es wird während des

Verbindungsaufbaus ausgehandelt.128 Bit Schlüssel bieten eine stärkere Verschlüsselung als 40 Bit Schlüssel.

Modus:

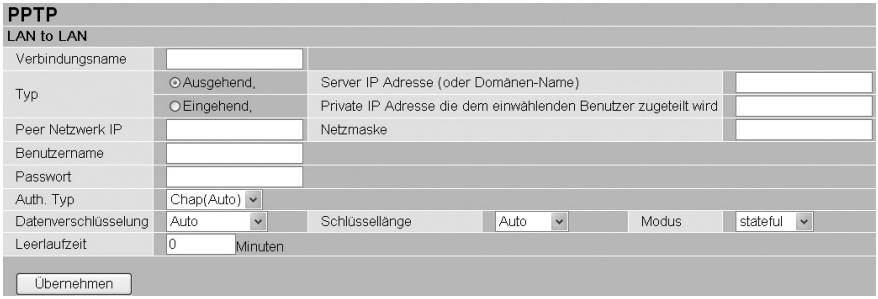
Sie können zwischen **Stateful** oder **Stateless** Modus wählen. Der Schlüssel wird alle 256 Pakets gewechselt wenn Sie Stateful Modus wählen. Wenn Sie Stateless Modus wählen, wechselt der Key in jedem Paket.

Leerlaufzeit:

Automatischer Verbindungsabbau bei VPN Verbindungen wenn keine Aktivität für eine voreingestellten Zeitraum stattfindet. 0 bedeutet die Verbindung ist immer aktiv.

Klicken Sie auf **Übermitteln** nachdem Sie die Veränderungen vorgenommen haben.

LAN zu LAN PPTP Verbindung



Verbindungsname:

Dies erlaubt Ihnen die diese spezielle Verbindung zu identifizieren, z.B.: „Verbindung zum Büro“.

Typ:

Klicken Sie **Ausgehend** wenn Sie wollen das Ihr Router als Client (verbindet zu einem entfernten VPN Server, z.B.: Ihr Büro Server), wählen Sie **Eingehend** arbeitet er als VPN Server.

- Wenn Ihr Router eine Verbindung zu einem entfernten LAN herstellen soll, geben Sie die **Server IP Adresse (oder Hostname)** ein mit der Sie sich verbinden wollen.

- Wenn Ihr Router als Server arbeiten soll, der hereinkommende Verbindungen akzeptiert, konfigurieren Sie die **Private IP Adresse die dem einwählenden Benutzer zugeordnet wird.**

Peer Netzwerk IP:

Geben Sie die Teilnehmer Netzwerk IP Adresse ein.

Netzmaske:

Geben Sie die Netzmaske ein des Teilnehmer Netzwerkes ein basierend auf die Teilnehmer Netzwerk IP.

Benutzername:

Wenn Sie ein Ausgehender Nutzer sind (Client), geben Sie den Benutzernamen ein der Ihnen vom Host gegeben wurde. Wenn Sie ein Eingehender Nutzer (server) sind, geben Sie Ihren eigenen Benutzernamen an.

Passwort:

Wenn Sie ein Ausgehender Nutzer sind (Client), geben Sie Ihr Passwort ein das Ihnen vom Host gegeben wurde. Wenn Sie ein Eingehender Nutzer (server) sind, geben Sie Ihr eigenes Passwort an.

Auth. Typ:

Standardwert ist **Auto,** wenn Sie wollen, das der Router den Authentication Typ selber erkennen soll oder aber wenn es CHAP (Challenge Handshake Authentication Protocol) oder PAP (Password Authentication Protocol) ist und Sie wissen welcher Typ vom Server benutzt wird. Wenn PAP benutzt wird, wird das Passwort unverschlüsselt gesendet, wobei CHAP das Passwort verschlüsselt, bevor es gesendet wird und auch es zu unterschiedlichen Momenten anfordert, um zu prüfen ob der Client nicht durch einen Eindringling ersetzt wurde

Datenverschlüsselung:

Daten die über die VPN Verbindung gesendet werden, können mit einem MPPE Algorithmus verschlüsselt werden. Standardwert ist **Auto,** so das die Einstellung während des Verbindungsaufbaus ausgetauscht werden oder aber Sie können die Verschlüsselung auf **Aktiviert** oder **Deaktiviert** setzen.

Schlüssellänge:

Die Daten werden mit einem MPPE Algorithmus mit 40 Bit oder 128 Bit verschlüsselt. Standardwert ist **Auto,** es wird während des Verbindungsaufbaus ausgehandelt.128 Bit Schlüssel bieten eine stärkere Verschlüsselung als 40 Bit Schlüssel.

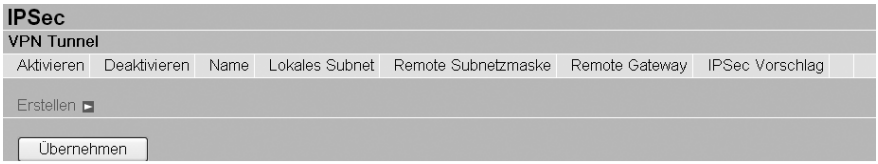
Modus:

Sie können zwischen **Stateful** oder **Stateless** Modus wählen. Der Schlüssel wird alle 256 Pakets gewechselt wenn Sie Stateful Modus wählen. Wenn Sie Stateless Modus wählen, wechselt der Key in jedem Packet.

Leerlaufzeit:

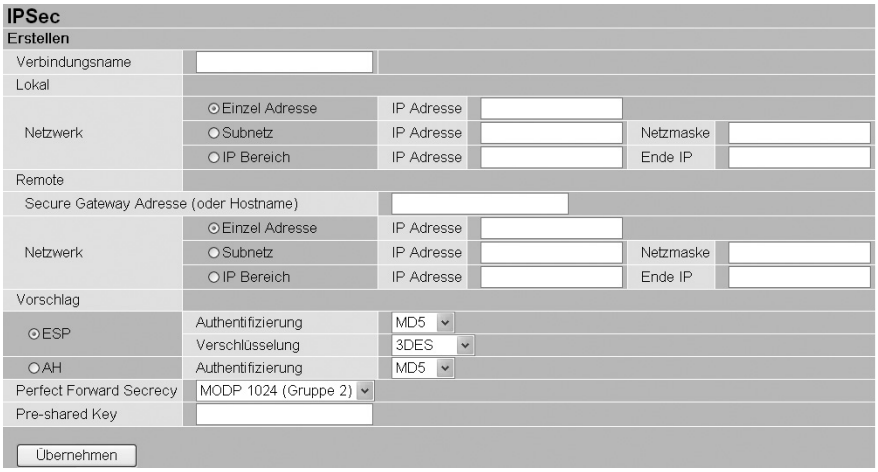
Automatischer Verbindungsabbau bei VPN Verbindungen wenn keine Aktivität für eine voreingestellten Zeitraum stattfindet. 0 bedeutet die Verbindung ist immer aktiv.
Klicken Sie auf **Übermitteln** nachdem Sie die Veränderungen vorgenommen haben.

IPSec



Klicken Sie auf **Erstellen** um eine neue IPSec VPN Verbindung zu erstellen.

Konfiguration einer IPSec VPN Verbindung



Verbindungsname: Dies erlaubt Ihnen die diese spezielle Verbindung zu identifizieren, z.B.: „Verbindung zum Büro“.

Lokal:

Lokal Netzwerk:

Geben Sie die IP Adresse, Subnetz Maske oder IP Bereich des lokalen Netzwerks an.

- Single Address: Die IP Adresse des lokalen Host.
- Subnetzmaske: Die Subnetzmaske des lokalen Netzwerk. Zum Beispiel IP: 192.168.2.0 mit der Netzmaske 255.255.255.0 spezifiziert ein Klasse C Subnetz welches von 192.168.2.1 bis 192.168.2.254 reicht.

- IP Bereich: Der IP Bereich des lokalen Netzwerk. Zum Beispiel IP: 192.168.2.1, End IP: 192.168.2.10

Remote:

Gateway Adresse (oder Hostname):
Die IP Adresse oder Hostname des entfernten VPN Geräts welches verbunden ist und einen VPN Tunnel aufbaut.

Network:
Legt die IP Adresse, Subnetz oder den IP Bereich des Remote Netzwerkes fest.

Vorschlag:
Wählen Sie die IPSec Sicherheitsmethode aus. Es gibt zwei Methoden die Authentifikation zu überprüfen, AH (authentication header) und ESP (Encapsulating Security Payload). Benutzen Sie ESP für größere Sicherheit, so das die Daten verschlüsselt und authentifiziert werden. Wenn Sie AH benutzen werden die Daten authentifiziert aber nicht verschlüsselt.

Authentifizierung:
Authentifizierung sichert die Integrität der Daten und verhindert ein verfälschen während des Transports. Es gibt drei Optionen, Message Digest 5 **(MD5)**, Secure Hash Algorithm **(SHA-1)** oder **NONE.** SHA-1 ist weitaus resistenter gegenüber brute-force Angriffen als MD5, aber es ist langsamer.

- **MD5:** Ein Einweg “hashing Algorithmus” der 128-Bit produziert.
- **SHA-1:** Ein Einweg “hashing Algorithmus” der 160-Bit produziert.

Verschlüsselung:
Wählen Sie die Verschlüsselungsmethode aus dem Pull-Down Menü. Es gibt vier Optionen, **DES, 3DES, AES** und **NONE.** NONE bedeutet es ist ein Tunnel ohne Verschlüsselung. 3DES und AES sind weitaus stärker, aber vermindern die Latenz.

- **DES:** Steht für Data Encryption Standard, es benutzt 56 Bits als Verschlüsselungsmethode.

- **3DES:** Steht für Triple Data Encryption Standard, es benutzt 168 (56*3) Bits als Verschlüsselungsmethode.

- **AES:** Steht für Advanced Encryption Standards, es benutzt 128 Bits als Verschlüsselungsmethode.

Perfect Forward Secrecy:

Wählen Sie PFS mit Diffie-Hellman public-key Kryptografie um die Zugangsschlüssel während der zweiten Phase der VPN Verhandlung zu aktivieren. Diese Funktion bietet eine höhere Sicherheit, aber verlängert die Verhandlungsphase von VPN. Diffie-Hellman ist ein public-key Kryptographie Protokoll welches zwei Teilnehmern erlaubt, eine sichere Verbindung über einen unsicheren Kommunikationskanal zu teilen. (z.B. Über das Internet). Es gibt drei Modes, MODP 768-Bit, MODP 1024-Bit und MODP 1536-Bit. MODP steht für Modular Exponentiation Groups.

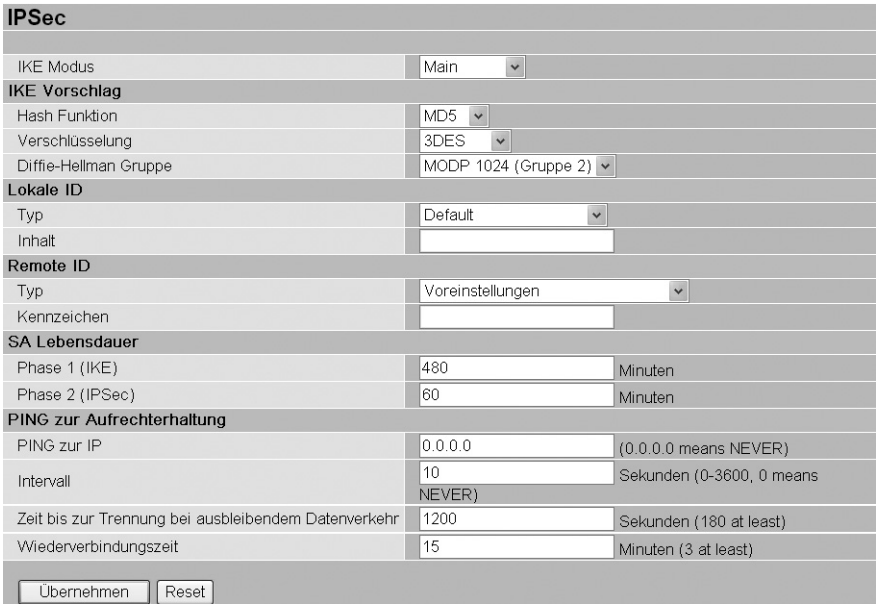
Pre-shared Key:

Dies ist für das Internet Key Exchange (IKE) Protokoll, ein String von 4 bis 128 Zeichen. Beide Seiten sollen den gleichen Key nutzen. IKE wird benutzt, um eine sichere Verbindung aufzubauen und ein authentifizierter Key für Service (wie IPSec) welches einen Key benötigt. Bevor irgendwelcher IPSec Verkehr durchgeführt wird, wird die Richtigkeit der jeweiligen Router Gegenstation überprüft. Dies kann manuell geschehen wenn Sie den Pre-Shared Key auf beiden Seiten eingeben (Router oder host).

Klicken Sie auf den **Übernehmen** Button um die Einstellungen zu speichern.

Erweiterte Optionen

Klicken Sie auf Erweiterte Optionen um die folgenden Einstellen zu ändern:



IKE Mode: Wählen Sie den IKE Modus auf Main Modus oder Agressive Modus.

Lokale ID:

- Type: Geben Sie den lokalen ID Typ an.
- Content: Geben Sie die ID Information ein, wie www.ipsectest.com.

Remote ID:

- Type: Geben Sie den entfernten ID Typ ein.
- Identifier: Geben Sie die entferne ID Information ein, wie **www.ipsectest.com.**

SA Lifetime:

Gibt die Zeit in Minuten an, die eine Security Association (SA) aktiv bleibt, bevor eine neue Verschlüsselung und Authentifizierungsschlüssel ausgetauscht werden. Es gibt zwei Arten von SAs, IKE und IPSec. IKE verhandelt und führt SA im Auftrag von IPSec, ein IKE SA wird von IKE benutzt.

Phase 1 (IKE):

Um eine Eingangsverbindung für einen VPN Tunnel aufzubauen,

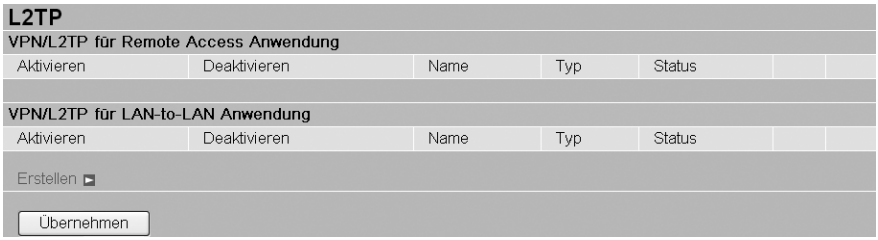
kann die mögliche Reichweite von 5 bis 15000 Minuten sein, der Standardwert ist 240 Minuten.

Phase 2 (IPSec):
Um eine sichere Authentifikation herzustellen. Die mögliche Reichweite ist von 5 bis 15000 Minuten, der Standardwert ist 60 Minuten.

Eine kurze SA Zeit verbessert die Sicherheit da beide Gegenseiten gezwungen sind die Schlüssel zu aktualisieren. Jedes Mal wenn ein VPN Tunnel erneuert wird, wird der Zugang durch den Tunnel kurzfristig abgebrochen.

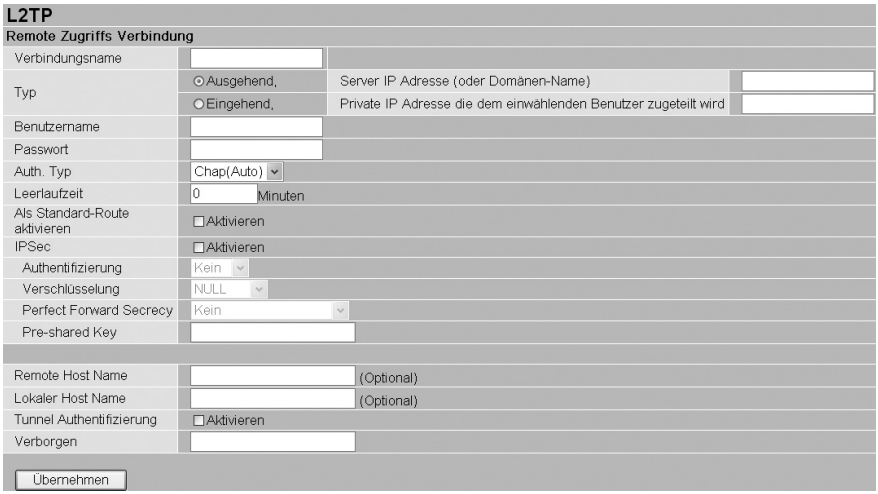
Klicken Sie den **Übermitteln** Button um die Einstellungen zu aktualisieren.

L2TP



Es gibt zwei Typen die L2TP VPN unterstützt, Remote Zugriff und LAN-to-LAN. (schauen Sie weiter unten für mehr Informationen. Klicken Sie auf **Erstellen** um eine neue VPN Verbindung zu konfigurieren.

Remote Zugriffs L2TP Verbindung



Verbindungsname:

Dieses erlaubt Ihnen die Verbindung zu identifizieren, z.B. “Verbindung zum Büro”.

Typ:

Klicken Sie Ausgehend an, wenn der Router als Client arbeiten soll (Verbindung zu einem Remote VPN Server, z.B. Ihren Büro Server), klicken Sie Eingehend wenn er als VPN Server arbeitet.

- Wenn Ihr Router eine Verbindung zu einem entfernten LAN herstellen soll, geben Sie die Server IP Adresse (oder Hostname) ein mit der Sie sich verbinden wollen.

- Wenn Ihr Router als Server arbeiten soll, der hereinkommende Verbindungen akzeptiert, konfigurieren Sie die Private IP Adresse die dem einwählenden Benutzer zugeordnet wird.

Benutzername:

Wenn Sie ein Ausgehender Nutzer sind (client), geben Sie den Benutzernamen ein der Ihnen vom Host gegeben wurde. Wenn Sie ein Eingehender Nutzer (server) sind, geben Sie Ihren eigenen Benutzernamen an.

Passwort:

Wenn Sie ein Ausgehender Nutzer sind (client), geben Sie Ihr Passwort ein das Ihnen vom Host gegeben wurde. Wenn Sie ein Eingehender Nutzer (server) sind, geben Sie Ihr eigenes Passwort an.

Auth. Typ:

Standardwert ist **Auto,** wenn Sie wollen, das der Router den Authentication Typ selber erkennen soll oder aber wenn es CHAP (Challenge Handshake Authentication Protocol) oder PAP (Password Authentication Protocol) ist und Sie wissen welcher Typ vom Server benutzt wird. Wenn PAP benutzt wird, wird das Passwort unverschlüsselt gesendet, wobei CHAP das Passwort verschlüsselt, bevor es gesendet wird und auch es zu unterschiedlichen Momenten anfordert, um zu prüfen ob der Client nicht durch einen Eindringling ersetzt wurde.

Leerlaufzeit Timer:

Automatischer Verbindungsabbau der VPN Verbindung wenn für einen vorgegebene Zeit keine Aktivität vorliegt. 0 bedeutet das die Verbindung immer besteht.

Klicken Sie auf **Übermitteln** nachdem Sie die Veränderungen vorgenommen haben.

IPSec:

Aktivieren, um eine verbesserte Sicherheit für L2TP VPN zu bekommen.

Authentifizierung:

Authentifizierung sichert die Integrität der Daten und verhindert ein verfälschen während des Transports. Es gibt drei Optionen, Message Digest 5 **(MD5),** Secure Hash Algorithm **(SHA-1)** oder **NONE.** SHA-1 ist weitaus resistenter gegenüber brute-force Angriffen als MD5, aber es ist langsamer.

- **MD5:** Ein Einweg “hashing Algorithmus” der 128-Bit produziert.
- **SHA-1:** Ein Einweg “hashing Algorithmus” der 160-Bit produziert.

Verschlüsselung:

Wählen Sie die Verschlüsselungsmethode aus dem Pull-Down Menü. Es gibt vier Optionen, **DES, 3DES, AES** und **NONE.** NONE bedeutet es ist ein Tunnel ohne Verschlüsselung. 3DES und AES sind weitaus stärker, aber vermindern die Latenz

- **DES:** Steht für Data Encryption Standard, es benutzt 56 Bits als Verschlüsselungsmethode.
- **3DES:** Steht für Triple Data Encryption Standard, es benutzt 168 (56*3) Bits als Verschlüsselungsmethode.
- **AES:** Steht für Advanced Encryption Standards, es benutzt 128 Bits als Verschlüsselungsmethode.

Perfect Forward Secrecy:

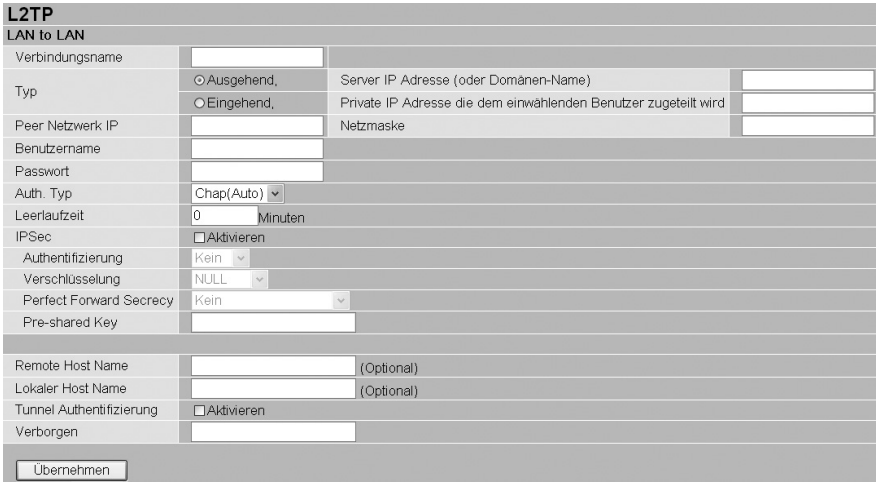
Wählen Sie PFS mit Diffie-Hellman public-key Kryptografie um die Zugangsschlüssel während der zweiten Phase der VPN Verhandlung zu aktivieren. Diese Funktion bietet eine höhere Sicherheit, aber verlängert die Verhandlungsphase von VPN. Diffie-Hellman ist ein public-key Kryptographie Protokoll welches zwei Teilnehmern erlaubt, eine sichere Verbindung über einen unsicheren Kommunikationskanal zu teilen. (z.B. Über das Internet). Es gibt drei Modes, MODP 768-Bit, MODP 1024-Bit und MODP 1536-Bit. MODP steht für Modular Exponentiation Groups.

Pre-shared Key:

Dies ist für das Internet Key Exchange (IKE) Protokoll, ein String von 4 bis 128 Zeichen. Beide Seiten sollen den gleichen Key nutzen. IKE wird benutzt, um eine sichere Verbindung aufzubauen und ein authentifizierter Key für Service (wie IPSec) welches einen Key benötigt. Bevor irgendwelcher IPSec Verkehr durchgeführt wird, wird die Richtigkeit der jeweiligen Router Gegenstation überprüft. Dies kann manuell geschehen wenn Sie den Pre-Shared Key auf beiden Seiten eingeben (Router oder host).

Klicken Sie auf den **Übernehmen** Button um die Einstellungen zu speichern.

LAN zu LAN L2TP Verbindung



Verbindungsname:

Dieses erlaubt Ihnen die Verbindung zu identifizieren.

Typ:

Klicken Sie **Ausgehend** an, wenn der Router als Client arbeiten soll (Verbindung zu einem Remote VPN Server, z.B. Ihren Büro Server), klicken Sie **Eingehend** wenn er als VPN Server arbeitet.

- Wenn Ihr Router eine Verbindung zu einem entfernten LAN herstellen soll, geben Sie die **Server IP Adresse (oder Hostname)** ein mit der Sie sich verbinden wollen.

- Wenn Ihr Router als Server arbeiten soll, der hereinkommende Verbindungen akzeptiert, konfigurieren Sie die **Private IP Adresse die dem einwählenden Benutzer zugeordnet wird.**

Teilnehmer Netzwerk IP:

Geben Sie die Teilnehmer Netzwerk IP Adresse ein.

Netzmaske:

Geben Sie die Netzmaske ein des Teilnehmer Netzwerkes ein basierend auf die Teilnehmer Netzwerk IP.

Benutzername:

Wenn Sie ein Ausgehender Nutzer sind (client), geben Sie den Benutzernamen ein der Ihnen vom Host gegeben wurde. Wenn Sie ein Eingehender Nutzer (server) sind, geben Sie Ihren eigenen Benutzernamen an.

Passwort::

Wenn Sie ein Ausgehender Nutzer sind (client), geben Sie Ihr Passwort ein das Ihnen vom Host gegeben wurde. Wenn Sie ein Eingehender Nutzer (server) sind, geben Sie Ihr eigenes Passwort an.

Auth. Typ:

Standardwert ist **Auto,** wenn Sie wollen, das der Router den Authentication Typ selber erkennen soll oder aber wenn es CHAP (Challenge Handshake Authentication Protocol) oder PAP (Password Authentication Protocol) ist und Sie wissen welcher Typ vom Server benutzt wird. Wenn PAP benutzt wird, wird das Passwort unverschlüsselt gesendet, wobei CHAP das Passwort verschlüsselt, bevor es gesendet wird und auch es zu unterschiedlichen Momenten anfordert, um zu prüfen ob der Client nicht durch einen Eindringling ersetzt wurde.

Leerlaufzeit Timer:

Automatischer Verbindungsabbau der VPN Verbindung wenn für einen vorgegebene Zeit keine Aktivität vorliegt. 0 bedeutet das die Verbindung immer besteht. Klicken Sie auf **Übermitteln** nachdem Sie die Veränderungen vorgenommen haben.

IPSec:

Aktivieren, um eine verbesserte Sicherheit für L2TP VPN zu bekommen.

Authentifizierung:

Authentifizierung sichert die Integrität der Daten und verhindert ein verfälschen während des Transports. Es gibt drei Optionen, Message Digest 5 **(MD5),** Secure Hash Algorithm **(SHA-1)** oder **NONE.** SHA-1 ist weitaus resistenter gegenüber brute-force Angriffen als MD5, aber es ist langsamer.

- **MD5:** Ein Einweg “hashing Algorithmus” der 128-Bit produziert.

- **SHA-1:** Ein Einweg “hashing Algorithmus” der 160-Bit produziert.

Verschlüsselung:

Wählen Sie die Verschlüsselungsmethode aus dem Pull-Down Menü. Es gibt vier Optionen, **DES, 3DES, AES** und **NONE.** NONE bedeutet es ist ein Tunnel ohne Verschlüsselung. 3DES und AES sind weitaus stärker, aber vermindern die Latenz.

- **DES:** Steht für Data Encryption Standard, es benutzt 56 Bits als Verschlüsselungsmethode.

- **3DES:** Steht für Triple Data Encryption Standard, es benutzt 168 (56*3) Bits als Verschlüsselungsmethode.

- **AES:** Steht für Advanced Encryption Standards, es benutzt 128 Bits als Verschlüsselungsmethode.

Perfect Forward Secrecy:

Wählen Sie PFS mit Diffie-Hellman public-key Kryptografie um die Zugangsschlüssel während der zweiten Phase der VPN Verhandlung zu aktivieren. Diese Funktion bietet eine höhere Sicherheit, aber verlängert die Verhandlungsphase von VPN. Diffie-Hellman ist ein public-key Kryptographie Protokoll welches zwei Teilnehmern erlaubt, eine sichere Verbindung über einen unsicheren Kommunikationskanal zu teilen. (z.B. Über das Internet). Es gibt drei Modes, MODP 768-Bit, MODP 1024-Bit und MODP 1536-Bit. MODP steht für Modular Exponentiation Groups.

Pre-shared Key:

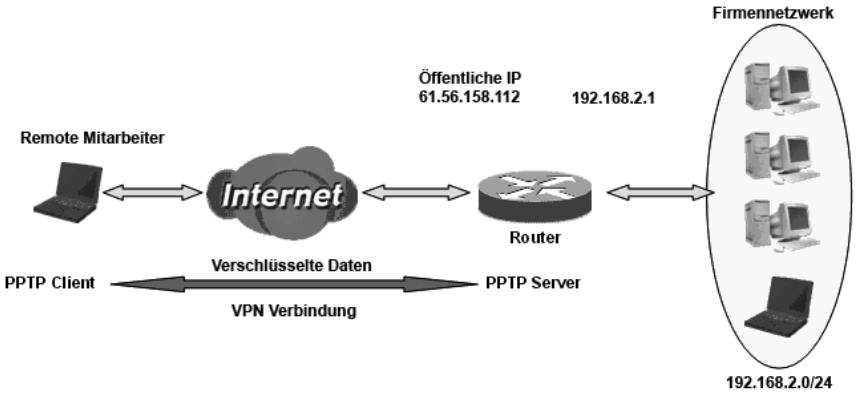
Dies ist für das Internet Key Exchange (IKE) Protokoll, ein String von 4 bis 128 Zeichen. Beide Seiten sollen den gleichen Key nutzen. IKE wird benutzt, um eine sichere Verbindung aufzubauen und ein authentifizierter Key für Service (wie IPSec) welches einen Key benötigt. Bevor irgendwelcher IPSec Verkehr durchgeführt wird, wird die Richtigkeit der jeweiligen Router Gegenstation überprüft. Dies kann manuell geschehen wenn Sie den Pre-Shared Key auf beiden Seiten eingeben (Router oder host).

Klicken Sie auf den **Übernehmen** Button um die Einstellungen zu speichern.

Beispiele VPN Konfiguration

Beispiel:
Konfiguration einer Fernzugriff PPTP VPN Einwahlverbindung

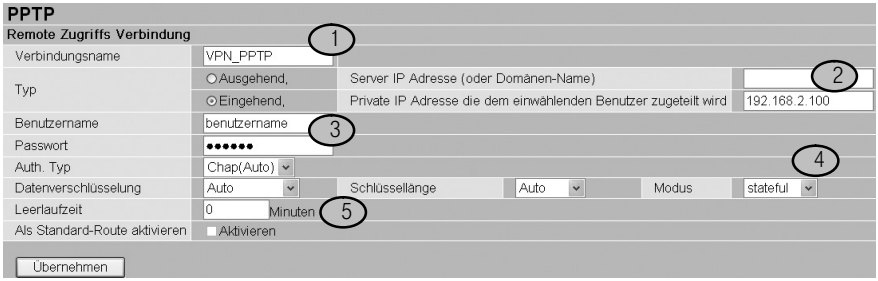
Ein entfernter Kollege richtet eine PPTP VPN Verbindung mit der Firma über Microsofts VPN Adapter (inklusive in Windows 2000/ME, etc.) Der Router ist in der Firma installiert, und verbindet einige PCs und Server.



PPTP VPN-Remote Zugriffs Verbindung (Eingehend)

Konfiguration PPTP VPN in der Firma

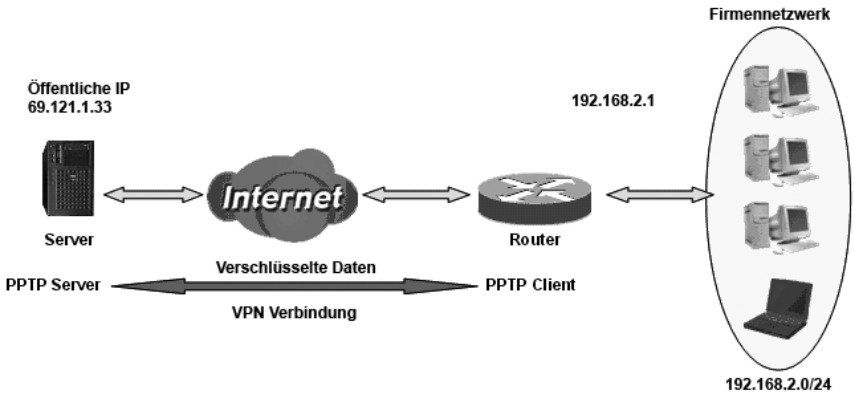
Die IP Adresse 192.168.2.200 wird dem Kollegen zugeordnet. Bitte prüfen Sie, daß diese IP nicht im Firmennetzwerk benutzt wird.



Item	Funktion		Beschreibung
1	Verbindungsname	VPN_PPTP	Verbindungsname
2	Eingehend		Eingehend
	Private IP Adresse, die dem einwählenden Benutzer zugeordnet wird.	192.168.2.200	Private IP Adresse, die dem einwählenden Benutzer zugeordnet wird.
3	Benutzername	Benutzername	Benutzername Passwort
	Passwort	xxxxxx	
4	Auth.Typ	Chap(Auto)	Auth.Typ Verschlüsselung Datenverschlüsselung Modus
	Verschlüsselung	Auto	
	Datenverschlüsselung	Auto	
	Modus	stateful	
5	Leerlaufzeit	0	Leerlaufzeit

Beispiel:
Konfiguration einer Fernzugriff PPTP VPN Dial-out Verbindung

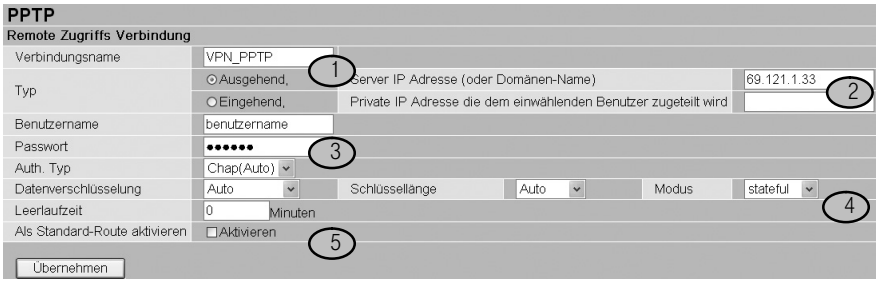
Ein Firmenbüro kann eine PPTP VPN Verbindung mit einem File Servern herstellen, der einen anderen Standort hat. Der Router ist in der Firma installiert, und verbindet einige PCs und Server.



PPTP VPN-Remote Zugriffs Verbindung (Ausgehend)

Konfiguration von PPTP VPN in der Firma

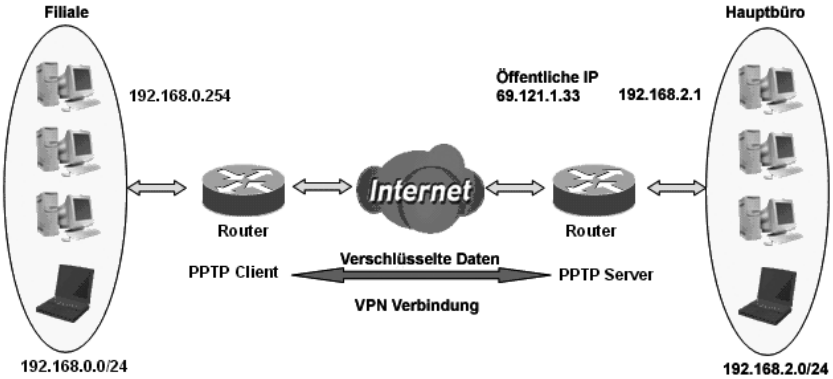
Sie können die IP Adresse eingeben (69.1.121.33 in diesem Fall) oder den Hostnamen, um den Server zu erreichen.



Item	Funktion		Beschreibung
1	Verbindungsname	VPN_PPTP	Verbindungsname
2	Ausgehend		Ausgehend
	Server IP Adresse (oder Hostname)	69.1.121.33	Server IP Adresse (oder Hostname)
3	Benutzername	Benutzername	Benutzername Passwort
	Passwort	xxxxxx	
4	Auth.Typ	Chap(Auto)	Auth.Typ Verschlüsselung Schlüssellänge Mode
	Verschlüsselung	Auto	
	Schlüssellänge	Auto	
	Mode	stateful	
5	Leerlaufzeit	0	Leerlaufzeit

Beispiel:
Konfiguration einer LAN-zu-LAN PPTP VPN Verbindung

Das Filialbüro stellt einen PPTP VPN Tunnel mit der Firma her, um zwei private Netzwerke über das Internet miteinander zu verbinden. Die Router sind jeweils in der Firma und im Filialbüro installiert.



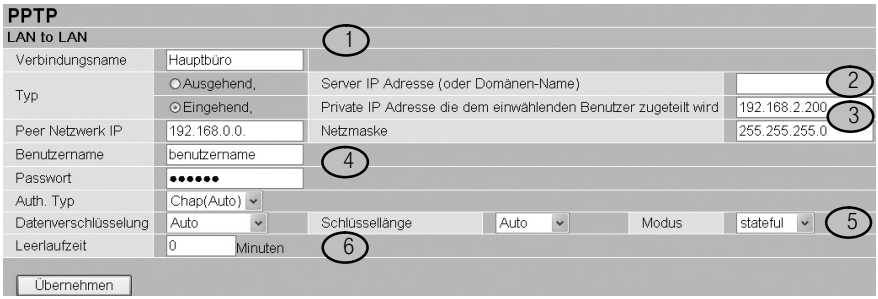
PPTP VPN-LAN zu LAN

Tipp

LAN Netzwerke müssen in unterschiedlichen Subnetzen sein bei LAN zu LAN Anwendungen.

Konfiguration PPTP VPN in der Firma

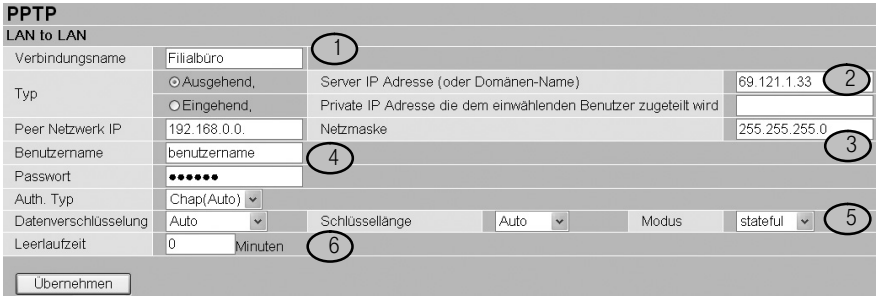
Die IP Adresse 192.168.2.201 wird dem Router im Filialbüro zugeordnet. Bitte überprüfen Sie, dass diese IP nicht im Firmennetzwerk benutzt wird.



Item	Funktion		Beschreibung
1	Verbindungsname	Hauptbüro	Verbindungsname
2	Eingehend		Eingehend
	Private IP Adresse, die dem einwählenden Benutzer zugeordnet wird	192.168.2.201	Private IP Adresse, die dem einwählenden Benutzer zugeordnet wird
3	Teilnehmer Netzwerk IP	192.168.0.0	Teilnehmer Netzwerk IP
	Netzmaske	255.255.255.0	Netzmaske
4	Benutzername	Benutzername	Benutzername
	Passwort	xxxxxx	Passwort
5	Auth.Typ	Chap(Auto)	Auth.Typ Datenverschlüsselung Schlüssellänge Modus
	Datenverschlüsselung	Auto	
	Schlüssellänge	Auto	
	Modus	stateful	
6	Leerlaufzeit	0	Leerlaufzeit

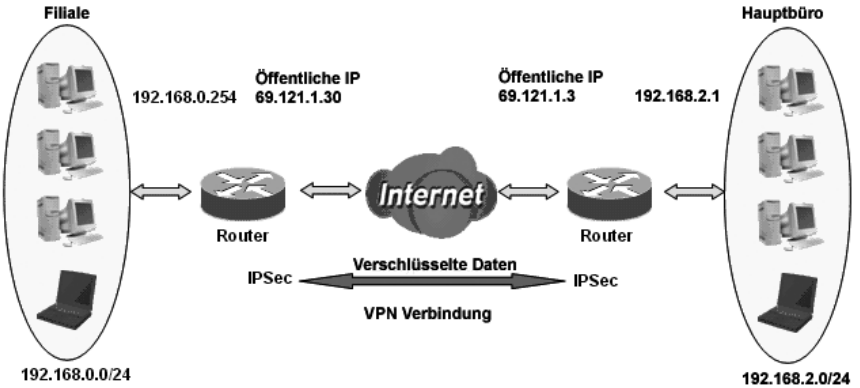
Konfiguration PPTP VPN im Filialbüro

Die IP Adresse 69.1.121.30 ist die **Public IP** Adresse des Routers in der Firma. Wenn Sie sich bei **DDNS** (schauen Sie im Abschnitt DDNS dieser Anleitung nach), können Sie anstelle der IP Adresse auch den Domain Namen angeben, um den Router zu erreichen.



	Funktion		Beschreibung
1	Verbindungsname	Filialbüro	Verbindungsname
2	Ausgehend		Ausgehend
	Server IP Adresse (oder Hostname)	69.1.121.3	Server IP Adresse (oder Hostname)
3	Teilnehmer Netzwerk IP	192.168.2.0	Teilnehmer Netzwerk IP Netzmaske
	Netzmaske	255.255.255.0	
4	Benutzername	Benutzername	Benutzername Passwort
	Passwort	xxxxxx	
5	Auth.Typ	Chap(Auto)	Auth.Typ Datenverschlüsselung Schlüssellänge Modus
	Datenverschlüsselung	Auto	
	Schlüssellänge	Auto	
	Modus	stateful	
6	Leerlaufzeit	0	Leerlaufzeit

Beispiel: Konfiguration einer IPSec LAN-zu-LAN VPN Verbindung



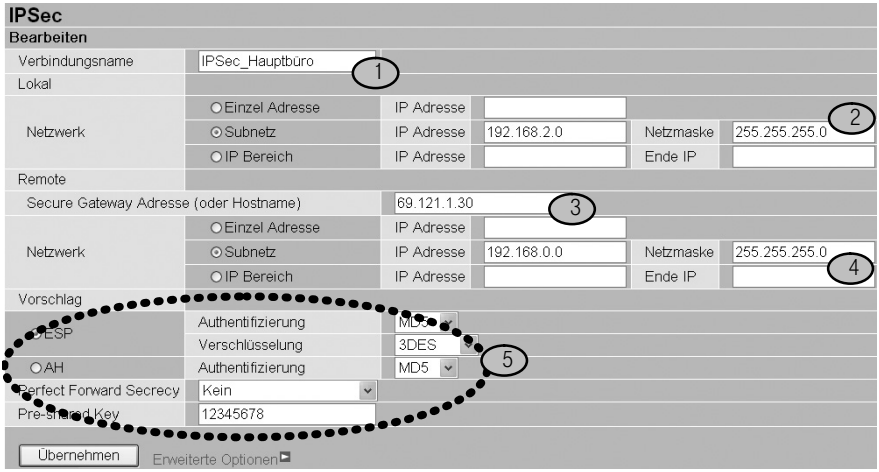
IPSec VPN-LAN zu LAN

Tabelle 3: Netzwerk Konfiguration und Sicherheitsplan		
	Filial Büro	Haupt Büro
Lokale Netzwerk ID	192.168.0.0/24	192.168.2.0/24
Lokale Router IP	69.1.121.30	69.1.121.3
Remote Netzwerk ID	192.168.2.0/24	192.168.0.0/24
Remote Router IP	69.1.121.3	69.1.121.30
IKE Pre-shared Key	12345678	12345678
VPN Verbindungs-Typ	Tunnel mode	Tunnel mode
Sicherheits- Algorithmus	ESP:MD5 mit AES	ESP:MD5 mit AES

Tipp

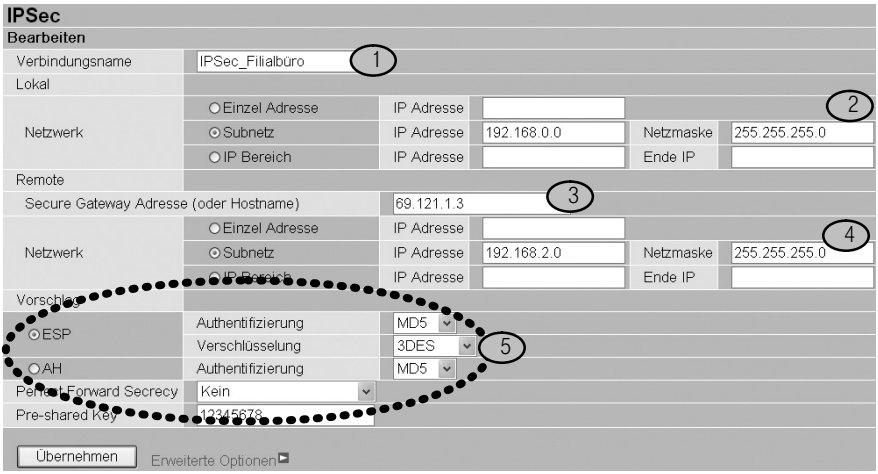
LAN Netzwerke müssen in unterschiedlichen Subnetzen sein bei LAN zu LAN Anwendungen. Die Funktionen des **Pre-shared Key, VPN Verbindungs-Typ und Sicherheits- Algorithmus** müssen auf beiden Seiten identisch sein.

Konfiguration von IPSec VPN im Hauptbüro



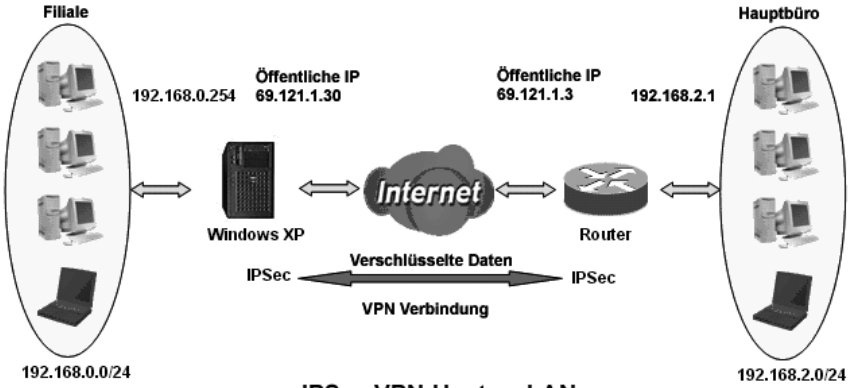
Item	Funktion		Beschreibung
1	Verbindungsname	IPSec_Hauptbüro	Gegebener Name der VPN Verbindung
2	Subnetz		Klicken Sie Subnetzmaske
	IP Adresse	192.168.2.0	Haupt Büro Netzwerk (siehe Tabelle 3)
	Netzmaske	255.255.255.0	
3	Secure Gateway Adresse (oder Hostname)	69.121.1.30	IP Adresse des Routers im Filialbüro (in WAN Seite)
4	Subnetz		Klicken Sie auf Subnetz-maske
	IP Adresse	192.168.0.0	Filialbüro Netzwerk (siehe Tabelle 3)
	Netzmaske	255.255.255.0	
5	ESP		
	Authentifizierung	MD5	Sicherheitsplan (siehe Ta-belle 3)
	Verschlüsselung	3DES	
	Perfect Forward Security	None	
	Pre-shared Key	12345678	

Konfiguration IPSec VPN in der Filiale



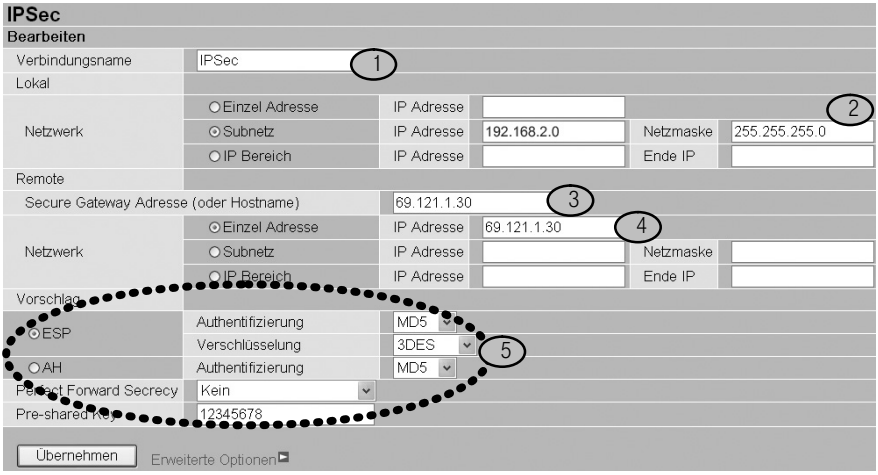
Item	Funktion		Beschreibung
1	Verbindungsname	IPSec_Filialbüro	Gegebener Name der VPN Verbindung
2	Subnetz		Klicken Sie Subnetzmaske
	IP Adresse	192.168.0.0	Filialbüro Netzwerk (siehe Tabelle 3)
	Netzmaske	255.255.255.0	
3	Secure Gateway Adresse (oder Hostname)	69.121.1.3	IP Adresse des Routers im Haupt Büro (in WAN Seite)
4	Subnetz		Klicken Sie auf Subnetz-maske
	IP Adresse	192.168.2.0	Haupt Büro Netzwerk (siehe Tabelle 3)
	Netzmaske	255.255.255.0	
5	ESP		Klicken Sie den ESP Button
	Authentifizierung	MD5	Sicherheitsplan (siehe Ta-belle 3)
	Verschlüsselung	3DES	
	Perfect Forward Security	Keiner	
	Pre-shared Key	12345678	

Beispiel:
Konfiguration einer IPSec Host-to-LAN VPN Verbindung



IPSec VPN-Host zu LAN

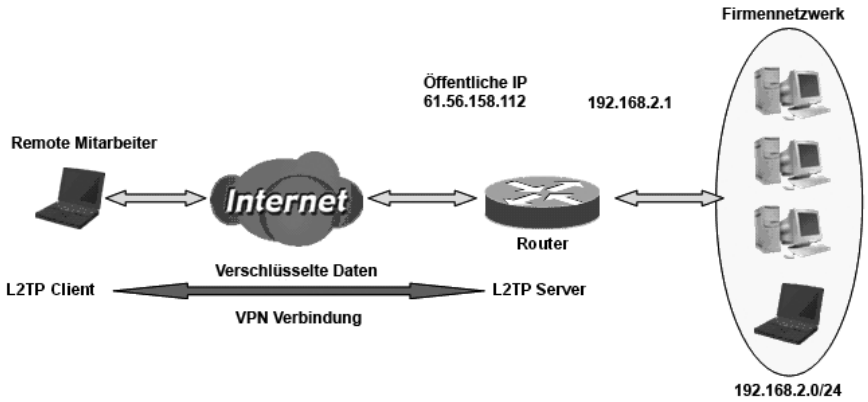
Konfiguration IPSec VPN im Hauptbüro



Item	Funktion		Beschreibung
1	Verbindungsname	IPSec	Gegebener Name der IPSec Verbindung
2	Subnetz		Klicken Sie Subnetzmaske
	IP Adresse	192.168.2.0	Hauptbüro Netzwerk
	Netzmaske	255.255.255.0	
3	Secure Gateway Adresse (oder Hostname)	69.121.1.30	IP Adresse des Hauptbüro Router (WAN seitig)
4	Einzel Adresse		Klicken Sie auf den Einzel Adressen Button
	IP Adresse	69.121.1.30	Entfernte IP Adresse des Kollegen
5	ESP		Klicken Sie den ESP Button
	Authentifizierung	MD5	
	Verschlüsselung	3DES	
	Perfect Forward Security	Keiner	
	Pre-shared Key	12345678	

Beispiel:
Konfiguration eines Remote Access L2TP VPN Dial-in Verbindung

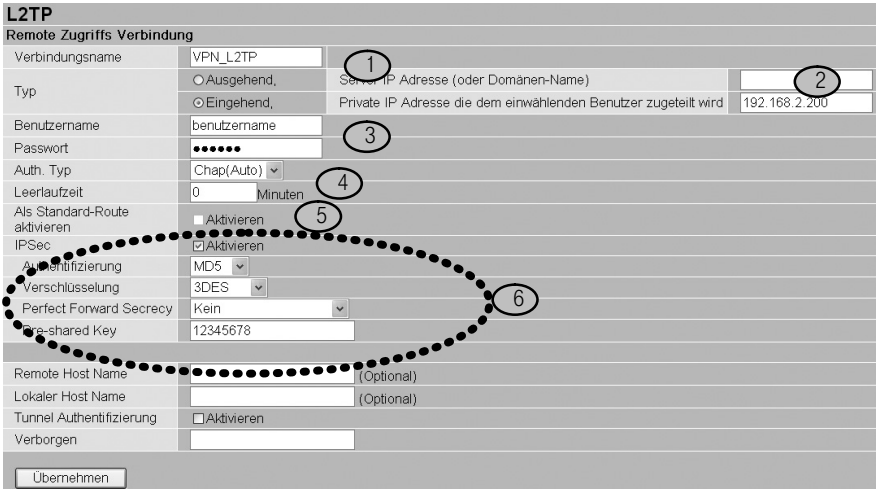
Ein entfernter Kollege stellt eine L2TP VPN Verbindung mit dem Hauptbüro her in dem er den Microsoft VPN Adapter benutzt (inklusive in Windows XP/2000/ME etc.). Der Router verbindet ein oder mehrere Rechner und Server im Hauptbüro miteinander.



L2TP VPN-Remote Zugriffs Verbindung (Eingehend)

Konfiguration von L2TP VPN im Hauptbüro

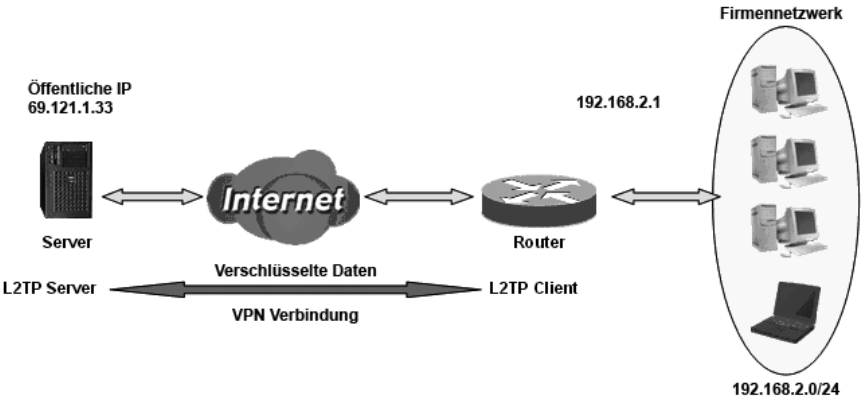
Die eingegebene IP Adresse 192.168.2.200 wird dem entfernten Kollegen zugeordnet. Vergewissern Sie sich das diese IP nicht im Büro LAN verwendet wird.



	Funktion		Beschreibung
1	Verbindungsname	VPN_L2TP	Name der L2TP Verbindung
2	Eingehend		Klicken Sie auf Eingehend
	Private IP Adresse die dem einwählenden Nutzer zugeordnet wird.	192.168.2.200	Die IP Adresse die dem einwählendem Kollegen zugeordnet wird.
3	Benutzername	Benutzername	Eingabe von Benutzername & Passwort um den entfernten Kollegen zu authentifizieren.
	Passwort	123456	
4	Auth.Typ	Chap(Auto)	Belassen Sie die Standardwerte hier in den meisten Fällen.
5	Leerlaufzeit	0	Die Verbindung wird getrennt sobald kein Verkehr für einen vordefinierten Zeitraum stattfindet. Leerlaufzeit 0 bedeutet die Verbindung besteht immer.
6	IPSec		Aktivieren für eine verbesserte L2TP VPN Sicherheit.
	Authentifizierung	MD5	Beide Seiten sollten die gleichen Werte benutzen.
	Verschlüsselung	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

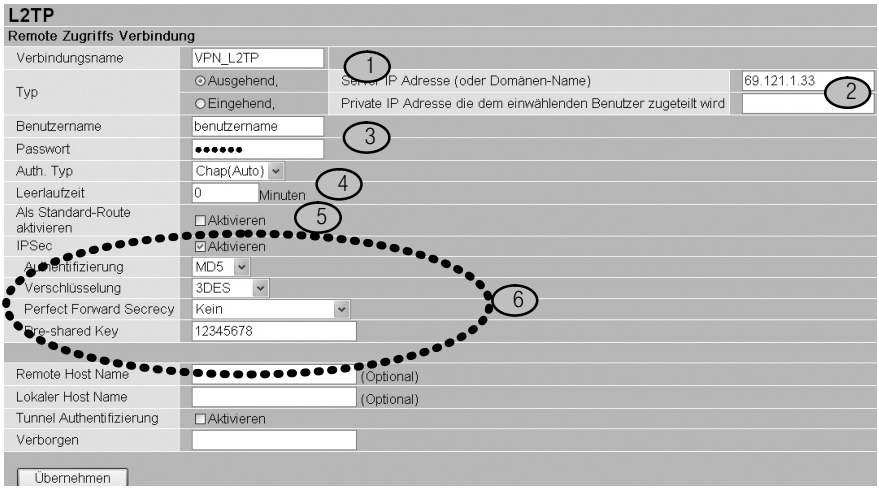
Beispiel:
Konfiguration einer Remote Access L2TP VPN Dial-out Verbindung

Ein Firmenbüro stellt eine L2TP VPN Verbindung mit einem File Server her der sich an einem anderen Standort befindet. Der Router im Firmenbüro verbindet mehrere PC und Server



L2TP VPN-Remote Zugriffs Verbindung (Ausgehend)

Konfiguration von L2TP VPN im Firmenbüro



	Funktion		Beschreibung
1	Verbindungsname	VPN_L2TP	Angegebener Name der L2TP Verbindung
2	Ausgehend		Klicken Sie Ausgehend an
	Server IP Adresse (oder Hostname)	69.121.1.33	Gewählte Server IP Adresse
3	Benutzername	Benutzername	Benutzername und Passwort
	Passwort	123456	
4	Auth.Typ	Chap(Auto)	Belassen Sie hier die Standardwerte in den meisten Fällen.
5	Leerlaufzeit	0	Die Verbindung wird getrennt sobald kein Verkehr für einen vordefinierten Zeitraum stattfindet. Leerlaufzeit 0 bedeutet die Verbindung besteht immer.
6	IPSec		Aktivieren für eine verbesserte L2TP VPN Sicherheit.
	Authentifizierung	MD5	Beide Seiten sollten die gleichen Werte benutzen.
	Verschlüsselung	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

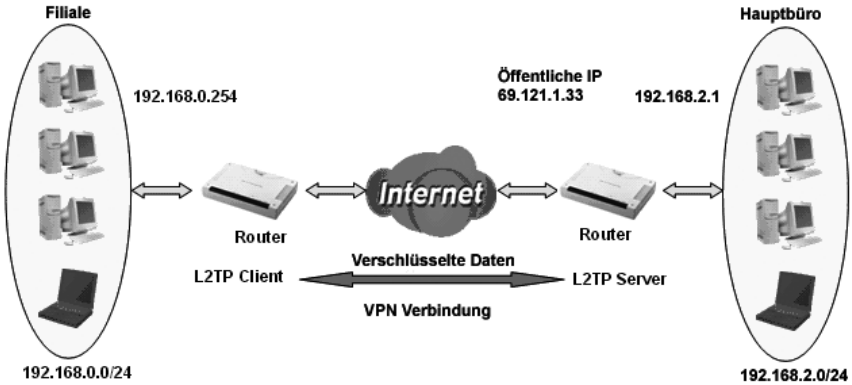
Beispiel: Konfiguration Ihres Routers zur Einwahl in den Server

Tipp

Momentan unterstützt Microsoft Windows Operation System keinen hereinkommenden L2TP Service. Zusätzliche Software wird dafür benötigt.

Beispiel: Konfiguration einer LAN-zu-LAN L2TP VPN Verbindung

Das Filialbüro stellt einen L2TP VPN Tunnel mit dem Hauptbüro her um zwei private Netzwerke über das Internet miteinander zu verbinden. Die Router sind jeweils im Filialbüro und Hauptbüro installiert.



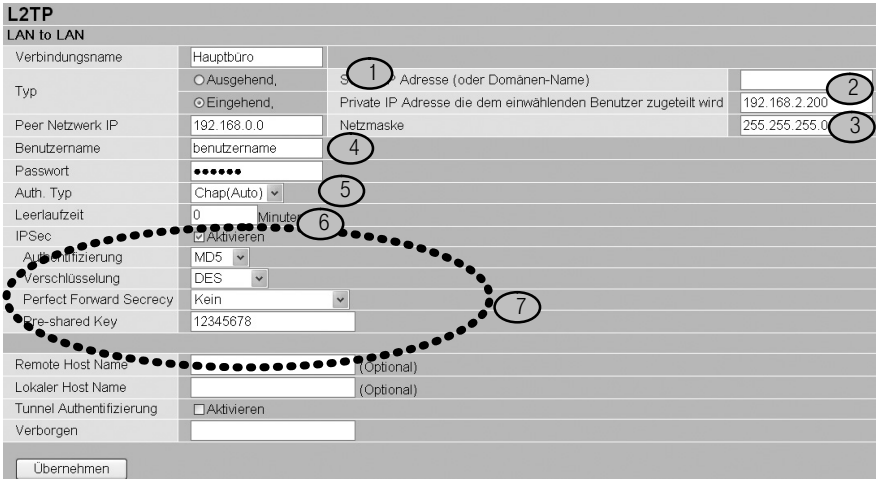
L2TP VPN-LAN zu LAN

Tipp

LAN Netzwerke müssen in unterschiedlichen Subnetzen sein bei LAN zu LAN Anwendungen. Die Funktionen des **Pre-shared Key, VPN Verbindungs-Typ und Sicherheits- Algorithmus** müssen auf beiden Seiten identisch sein.

Konfiguration von L2TP VPN im Hauptbüro

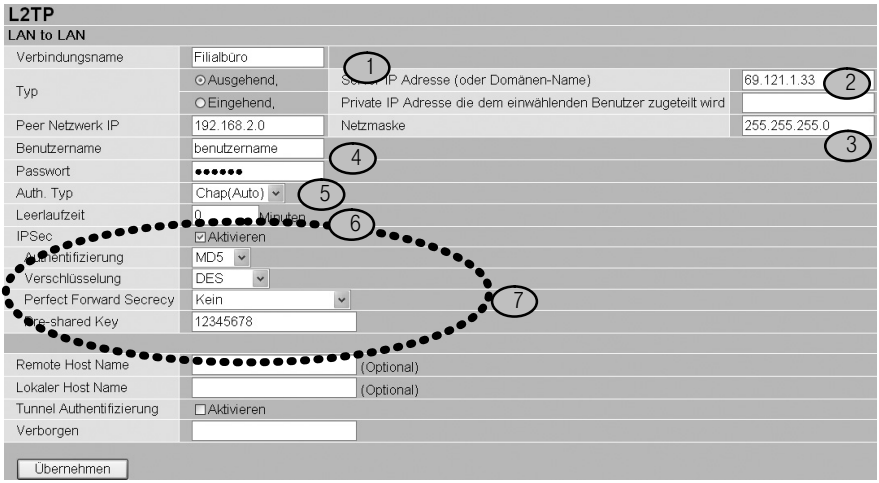
Die IP Adresse 192.168.2.200 wird dem Router im Filialbüro zugeordnet. Bitte vergewissern Sie sich das diese IP nicht im LAN des Hauptbüro benutzt wird.



	Funktion		Beschreibung
1	Verbindungsname	Hauptbüro	Gegebener Name der L2TP Verbindung
2	Eingehend		Klicken Sie Eingehend an
	Private IP Adresse die dem Nutzer zugeordnet wird.	192.168.2.200	IP Adresse die dem Filialbüro zugeordnet wird.
3	Teilnehmer Netzwerk IP	192.168.0.0	Filialbüro Netzwerk
	Netzmaske	255.255.255.0	
4	Benutzername	Benutzername	Eingabe von Benutzername & Passwort um sich als Filialbüro zu authentifizieren.
	Password	123456	
5	Auth.Typ	Chap(Auto)	Belassen Sie die Standardwerte in den meisten Fällen.
6	Leerlaufzeit	0	Die Verbindung wird getrennt, wenn kein Datenverkehr nach einer vordefinierten Zeit stattfindet. Leerlaufzeit 0 bedeutet ständig verbunden.
7	IPSec		Aktiveren um eine verbesserte L2TP VPN Sicherheit zu erhalten.
	Authentifizierung	MD5	
	Verschlüsselung	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	Beide Seiten sollten die gleichen Werte benutzen.

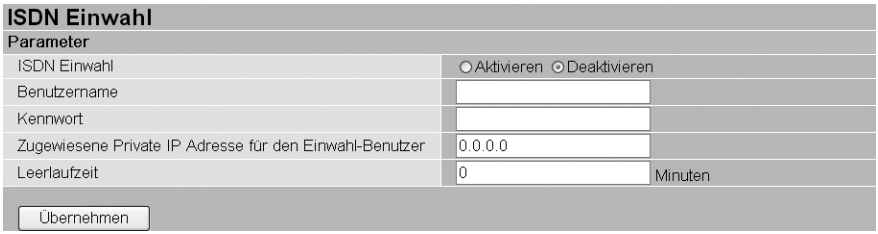
Konfiguration von L2TP im Filialbüro

Die IP Adresse 69.1.121.30 ist die öffentliche IP Adresse des Routers im Hauptbüro. Wenn Sie sich bei DDNS registriert haben (schauen Sie im Abschnitt DDNS dieser Anleitung nach) können Sie alternativ auch den Domain Namen anstelle der IP Adresse angeben.



	Funktion		Beschreibung
1	Verbindungsname	Filialbüro	Gegebener Name der L2TP Verbindung
2	Ausgehend		Klicken Sie auf Ausgehend
	Server IP Adresse (oder Hostname)	69.121.1.33	IP Adresse des Hauptbüro Router (WAN seitig)
3	Teilnehmer Netzwerk IP	192.168.2.0	Hauptbüro Netzwerk
	Netzmaske	255.255.255.0	
4	Benutzername	Benutzername	Eingabe von Benutzername & Passwort um sich als Filialbüro zu authentifizieren.
	Password	123456	
5	Auth.Typ	Chap(Auto)	Belassen Sie die Standardwerte in den meisten Fällen.
6	Leerlaufzeit	0	Die Verbindung wird getrennt, wenn kein Datenverkehr nach einer vordefinierten Zeit stattfindet. Leerlaufzeit 0 bedeutet ständig verbunden.
7	IPSec		Aktiveren um eine verbesserte L2TP VPN Sicherheit zu erhalten.
	Authentifizierung	MD5	
	Verschlüsselung	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	Beide Seiten sollten die gleichen Werte benutzen.

ISDN Einwahl



Hinweis: Diese Funktion ist hauptsächlich für Problemlösungen durch Ihren ISP gedacht.

ISDN Einwahl:

Werksseitig ist diese Funktion deaktiviert. Wenn Sie diese Funktion aktivieren agiert Ihr Router als ISDN Einwahl-Server und der Service Ihres ISP kann sich einwählen für eine Fernwartung.

Benutzername:

Der Benutzername für die Einwahl. Teilen Sie diesen dem Service Ihres ISP auf dessen Anfrage mit.

Passwort:

Das Passwort für die Einwahl. Teilen Sie dieses dem Service Ihres ISP auf dessen Anfrage mit.

Zugewiesene Private IP Adresse für den Einwahl-Benutzer:

Diese IP Adresse wird dem Einwahl-Benutzer zugewiesen. Bitte beachten Sie, dass diese IP Adresse in dem gleichen Subnetz wie die LAN IP Adresse des Routers sein muss.

Leerlaufzeit:

Automatischer Verbindungsabbau des Router wenn keine Aktivität für eine voreingestellte Zeit stattfindet.

QoS (Quality of Service)

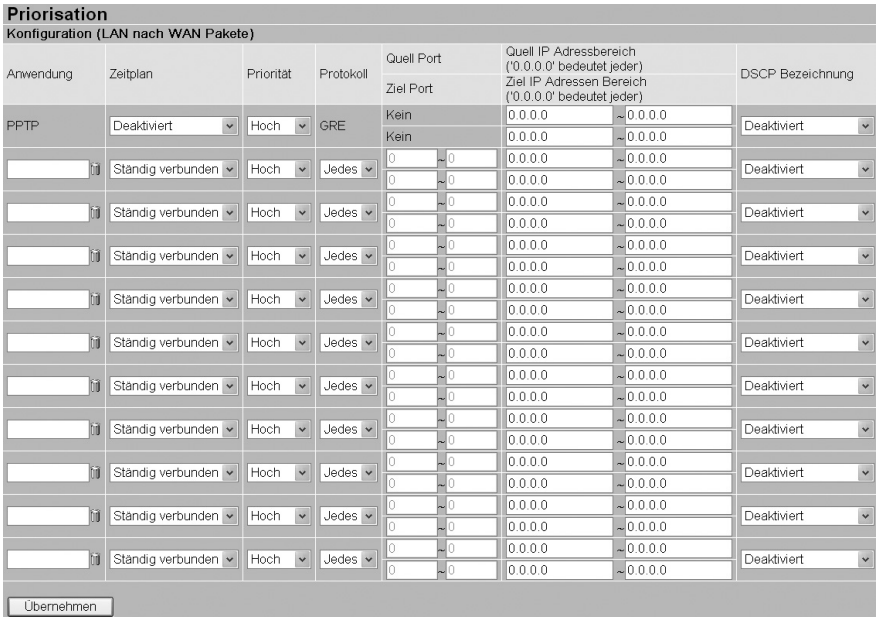
Die QoS Funktion hilft Ihnen, den Netzwerkverkehr für jedes Programm vom LAN (Ethernet und/oder Wireless) zum WAN (Internet) zu kontrollieren. Es ermöglicht Ihnen eine unterschiedliche Priorität und Datendurchsatz für jedes Programm zu konfigurieren, insbesondere wenn das System mit der vollen Upstream Geschwindigkeit arbeitet.
Sie finden drei Untermenüs unter QoS: **Priorisation, IP Throttling eingehend** und **IP Throttling ausgehend** (Bandbreitenmanagement).

Priorisation

Es gibt drei Priorisations Einstellungen, welche im Router angeboten werden:

- Hoch
- Normal (Werksseitig ist die normale Einstellung vorgegeben, ohne Priorisierung des Datenverkehrs.
- Niedrig

Die Balance der Ausnutzung jeder Priorität sind wie folgt eingestuft: Hoch (60%), Normal (30%) und Niedrig (10%).



Anwendung:

Der Name, der eine existierende Regel identifiziert.

Zeitplan:

Zeitvorgabe für die Regel.

Priorität:

Priorität für die Regel/Anwendung. Jeder Verkehr hat eine normale Priorität, so lange bis Sie dies ändern, also Hoch oder Niedrig einstellen.

Protokoll:

Der Name des zu verwenden Protokolles.

Quell Port:

Der Quell Port dessen Pakete überwacht werden.

Ziel Port:

Der Ziel Port dessen Pakete überwacht werden.

Quell IP Adressbereich:

Die Quell IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen.

Ziel IP Adressbereich:

Die Ziel IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen.

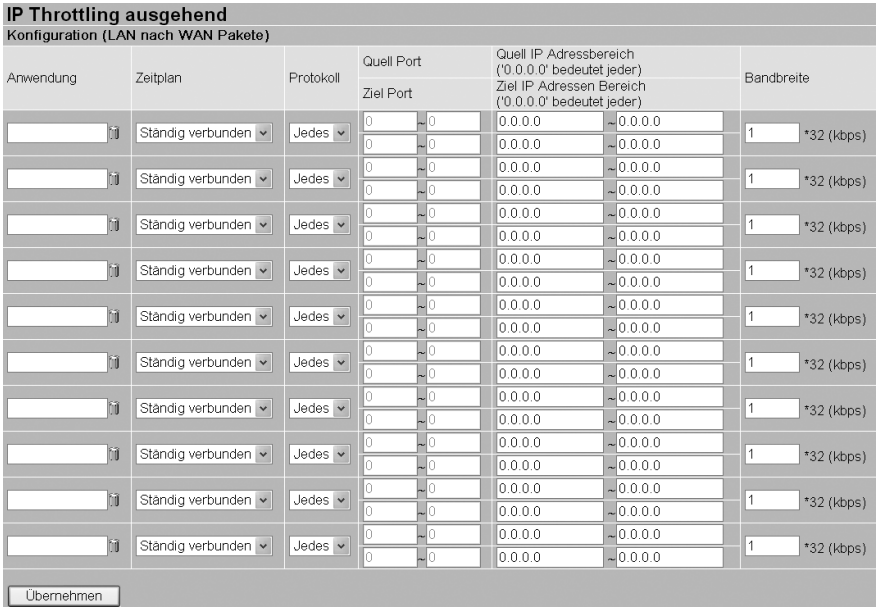
DSCP Bezeichnung:

Differentiated Services Code Point (DSCP), dies sind die ersten 6 Bits im ToS Byte. DSCP Marking erlaubt dem Anwender anhand des DSCP Wertes den Verkehr zu klassifizieren bevor die Pakete zum nächsten Router gesendet werden. Sehen Sie auch Tabelle 4.

Tabelle 4: DSCP Mapping Tabelle	
(Wireless) ADSL Router	Standard DSCP
Deaktiviert	Kein
Bestleistung	Bestleistung (000000)
Premium	Express Weiterleitung (101110)
Gold Service (L)	Class 1, Gold (001010)
Gold Service (M)	Class 1, Silber (001100)
Gold Service (H)	Class 1, Bronze (001110)
Silber Service (L)	Class 2, Gold (010010)
Silber Service (M)	Class 2, Silber (010100)
Silber Service (H)	Class 2, Bronze (010110)
Bronze Service (L)	Class 3, Gold (011010)
Bronze Service (M)	Class 3, Silber (011100)
Bronze Service (H)	Class 3, Bronze (011110)

IP Throttling ausgehend (LAN zum WAN)

IP Throttling erlaubt Ihnen die Geschwindigkeit des IP Verkehrs zu limitieren. Den Wert den Sie eintragen, multipliziert mit 32kbps, ergibt die limitierte Geschwindigkeit der Anwendung.



Anwendung:

Der Name, der eine existierende Regel identifiziert.

Zeitplan:

Zeitvorgabe für die Regel.

Priorität:

Priorität für die Regel/Anwendung. Jeder Verkehr hat eine normale Priorität, so lange bis Sie dies ändern, also Hoch oder Niedrig einstellen.

Protokoll:

Der Name des zu verwenden Protokolles.

Quell Port:

Der Quell Port dessen Pakete überwacht werden sollen.

Ziel Port:

Der Ziel Port dessen Pakete überwacht werden sollen.

Quell IP Adressbereich:

Die Quell IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen.

Ziel IP Adressbereich:

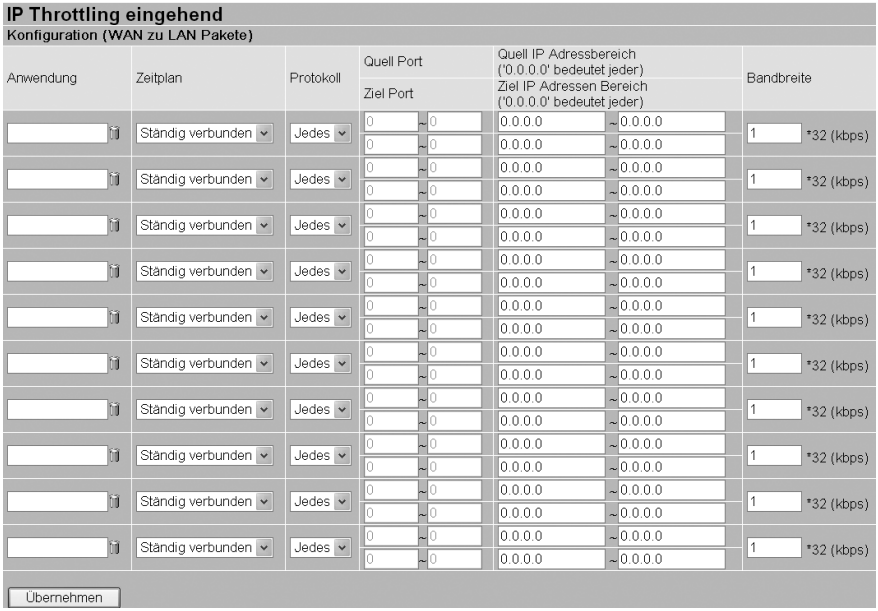
Die Ziel IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen.

Bandbreite:

Die limitierte Geschwindigkeit für den ausgehenden IP Verkehr.

IP Throttling eingehend (WAN zum LAN)

IP Throttling erlaubt Ihnen die Geschwindigkeit des IP Verkehrs zu limitieren. Den Wert den Sie eintragen, multipliziert mit 32kbps, ergibt die limitierte Geschwindigkeit der Anwendung.



Anwendung:

Der Name, der eine existierende Regel identifiziert.

Zeitplan:

Zeitvorgabe für die Regel.

Priorität:

Priorität für die Regel/Anwendung. Jeder Verkehr hat eine normale Priorität, so lange bis Sie dies ändern, also Hoch oder Niedrig einstellen.

Protokoll:

Der Name des zu verwenden Protokolles.

Quell Port:

Der Quell Port dessen Pakete überwacht werden.

Ziel Port:

Der Ziel Port dessen Pakete überwacht werden.

Quell IP Adressbereich:

Die Quell IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen.

Ziel IP Adressbereich:

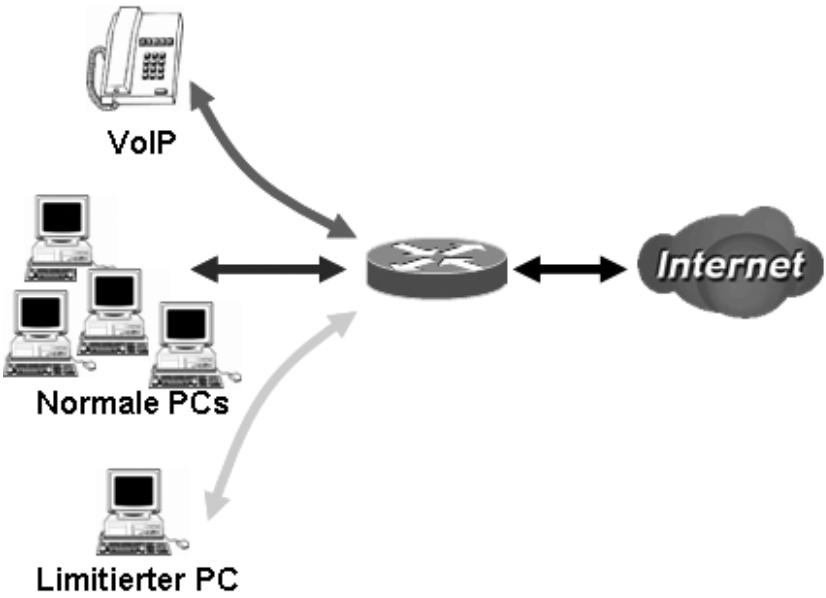
Die Ziel IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen.

Bandbreite:

Die limitierte Geschwindigkeit für den eingehenden IP Verkehr.

Beispiel:
QoS für Ihr Netzwerk

Verbindungs Diagramm



Information und Einstellungen

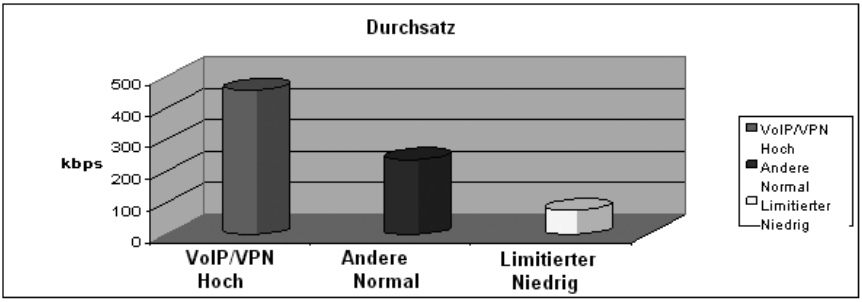
Upstream: 928 kbit/s
Downstream: 8 Mbit/s

VoIP Benutzer : 192.168.2.2
Normaler Benutzer : 192.168.2.3-192.168.2.5
Limitierter Benutzer : 192.168.2.100

Priorisation

Konfiguration (LAN nach WAN Pakete)

Anwendung	Zeitplan	Priorität	Protokoll	Quell Port / Ziel Port	Quell IP Adressbereich ('0.0.0.0' bedeutet jeder) / Ziel IP Adressen Bereich ('0.0.0.0' bedeutet jeder)	DSCP Bezeichnung
PPTP	Ständig verbunden	Hoch	GRE	Kein / Kein	0.0.0.0 ~ 0.0.0.0 / 0.0.0.0 ~ 0.0.0.0	Gold Service (L)
VoIP	Ständig verbunden	Hoch	Jedes	0 ~ 0 / 0 ~ 0	192.168.2.2 ~ 192.168.2.2 / 0.0.0.0 ~ 0.0.0.0	Gold Service (L)
Limitiert	TimeSlot1	Hoch	Jedes	0 ~ 0 / 0 ~ 0	192.168.2.100 ~ 192.168.2.100 / 0.0.0.0 ~ 0.0.0.0	Gold Service (L)



Missionskritische Anwendungen

Missionskritische Anwendungen müssen reibungslos gesendet werden ohne das Pakete verworfen werden. Setzen Sie hierfür die Priorität Hoch, damit andere Anwendungen nicht die Bandbreite belegen.

Sprach Anwendung

Sprach Anwendungen (VoIP) sind Latenz-Empfindlich. Die meisten VoIP Geräte verwenden das SIP Protokoll und die Port Nummer wird vom SIP Modul automatisch zugewiesen. Besser ist es feste IP Adressen für diese Geräte zu verwenden damit die VoIP Pakete eine hohe Priorität erhalten.

Die oben verwendeten Einstellungen verbessern die Qualität Ihres VoIP Dienstes auch bei hoher Last des Datenverkehrs.

Limitierte Anwendungen

Einige Firmen verwenden einen FTP Server für Ihre Kunden zum Download diverser Dateien oder Heimanwender verwenden FTP Server um Dateien auszutauschen.

Die oben verwendeten Einstellungen limitieren die Auslastung des Upstream vom FTP Server. Der Zeitplan unterstützt Sie des Weiteren dass diese Limitierung nur zu bestimmten Tageszeiten in Kraft tritt.

Erweiterte Einstellungen unter Verwendung von IP Throttling

Mittels IP Throttling können Sie Bandbreiten genauer zuteilen, selbst wenn die Anwendung den gleichen Status wie eine andere Anwendung hat.

Upstream: 928kbps (29*32kbps)

Missionskritische Anwendung: 192kbps (6*32kbps)

Sprach Anwendung: 128kbps (4*32kbps)

Limitierte Anwendung: 160kbps (5*32kbps)

Andere Anwendungen: 448kbps (14*32kbps)

6+4+14+5=29, 29*32kbps=928kbps

IP Throttling ausgehend

Konfiguration (LAN nach WAN Pakete)

Anwendung	Zeitplan	Protokoll	Quell Port / Ziel Port	Quell IP Adressbereich ('0.0.0.0' bedeutet jeder) / Ziel IP Adressen Bereich ('0.0.0.0' bedeutet jeder)	Bandbreite
PPTP	Ständig verbunden	gre	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	6 *32 (kbps)
VoIP	Ständig verbunden	Jedes	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	4 *32 (kbps)
Limitiert	TimeSlot1	Jedes	0 ~ 0 0 ~ 0	192.168.2.100 ~ 192.168.2.100 0.0.0.0 ~ 0.0.0.0	5 *32 (kbps)
Andere	TimeSlot1	Jedes	0 ~ 0 0 ~ 0	192.168.2.3 ~ 192.168.2.5 0.0.0.0 ~ 0.0.0.0	14 *32 (kbps)

Manchmal laden Ihre Kunden oder Freunde Dateien auf Ihren FTP Server und beeinträchtigen somit Ihren Downstream. Die Einstellungen unten helfen Ihnen die Bandbreite diesbezüglich zu limitieren.

IP Throttling eingehend

Konfiguration (WAN zu LAN Pakete)

Anwendung	Zeitplan	Protokoll	Quell Port / Ziel Port	Quell IP Adressbereich ('0.0.0.0' bedeutet jeder) / Ziel IP Adressen Bereich ('0.0.0.0' bedeutet jeder)	Bandbreite
Limitiert	TimeSlot1	Jedes	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 192.168.2.100 ~ 192.168.2.200	64 *32 (kbps)

Virtual Server (“Port Forwarding”)

In TCP/IP und UDP Netzwerken ist ein Port eine 16-Bit Nummer, welche benutzt wird, um ein Anwendungsprogramm zu identifizieren (normalerweise ein Server) wohin hereinkommende Verbindungen zugeordnet werden. Manche Anwendungen haben vordefinierte Ports von IANA (Internet Assigned Numbers Authority), und diese werden als “well-known ports” bezeichnet. Server folgen den „well-known port“ Zuordnungen, so dass Clients diese lokalisieren können. Wenn Sie einen Server auf Ihrem Netzwerk laufen lassen wollen, welcher vom WAN (z.B. von anderen Computern außerhalb Ihres Netzwerks) aus zugreifbar sein soll oder andere Programme, die hereinkommende Verbindungen akzeptieren (z.B. Peer-to-Peer/P2P Software wie Instant Messenger oder P2P File Sharing Programme) und NAT (Network Address Translation) nutzen, dann müssen Sie Ihren Router so konfigurieren, daß er die hereinkommenden Verbindungen an den entsprechenden Computer weiterleiten kann, auf dem dieses Programm läuft. Sie können ebenfalls Port Forwarding nutzen, wenn Sie einen Online Spiele Server hosten.

Der Grund dafür ist, wenn Sie NAT nutzen, daß Ihre öffentliche IP Adresse vom Router benutzt wird und auch dorthin zeigt, welcher allen Verkehr anschließend an die Private IP Ihrer PCs weiterleitet. Schauen Sie im Abschnitt WAN Konfiguration dieser Anleitung nach für weitere Informationen zu NAT.

Die Internet Assigned Numbers Authority (IANA) ist ein zentraler Koordinator für die Zuweisung der einzigartigen Parameterwerte für die Internet Protokolle. Port Nummern gehen von 0 bis 65535, aber nur Portnummern von 0 bis 1023 sind für privilegierte Services bestimmt und werden als “Well-Known Ports” bezeichnet. Die registrierten Ports sind von 1024 bis 49151 nummeriert. Die restlichen Ports werden als dynamische Ports oder private Ports bezeichnet, gehen von 49152 bis 65535.

Beispiele von Well-Known und registrierten Portnummern finden Sie in Tabelle 5, für weitere Informationen schauen Sie bitte nach auf:
http://www.iana.org/assignments/port-numbers

Der Router kann als Virtual Server konfiguriert werden, so dass externe Benutzer dienste wie WEB oder FTP Server über die öffentliche IP Adresse des Routers (WAN) automatisch zu dem Server in Ihrem LAN weitergeleitet werden, welcher weiterhin eine private IP Adresse hat.

Virtuellen Server hinzufügen

NAT kann als eine natürliche Firewall dienen, Ihr Router schützt Ihr Netzwerk vor Nutzung von fremden Personen, da alle hereinkommenden Verbindungen auf den Router zeigen, außer Sie nutzen einen Virtuellen Server, der die Einträge an PCs in Ihrem Netzwerk weiterleitet. Wenn Ihr Router anderen Internet Nutzern den Zugang zu Internen Servern erlauben soll, z.B. Webserver, Email Server, FTP Server oder Spielserver, fungiert der Router als ein Virtueller Server. Sie können einen lokalen Server mit einer speziellen Port Nummer diesen Service zuordnen z.B. web/HTTP (Port 80), FTP (Port 21), Telnet (Port 23), SMTP (Port 25), oder POP3 (Port 110), Wenn eine Anfrage von außerhalb an den Router kommt, leitet der Router die Anfrage an den dafür vorgesehenen internen Server weiter.

Zeitplan:

Hier können Sie einen selbst definierten Zeitplan für die Aktivierung Ihres Virtuellen Servers angeben. Wählen Sie den Zeitplan aus oder Ständig verbunden für den Virtuellen Server. Für die Einstellungen und weitere Information zum Zeitplan sehen Sie im Abschnitt Zeitplan nach.

Anwendung:

Tragen Sie hier einen Namen für die Anwendung ein oder klicken Sie auf Assistent um einen vorgegebene Anwendung auszuwählen.

Assistent :

20 vorgegebene Regeln haben Sie zur Auswahl. Wählen Sie eine

Anwedung aus werden die Anwendung, das Protokoll sowie die externen und umgeleiteten Ports in die entsprechenden Felder übernommen.

Protokoll:

Das für den Virtuellen Server zu verwendende Protokoll. Zusätzlich zu dem benötigten Port müssen Sie auch das benötigte Protokoll angeben. Welches Protokoll wird von der Anwendung festgelegt. Die meisten Anwendungen verwenden TCP oder UDP.

Externer Port:

Die Port Nummer welche auf der Remote/WAN Seite für den Virtuellen Server verwendet wird.

Umgeleiteter Port:

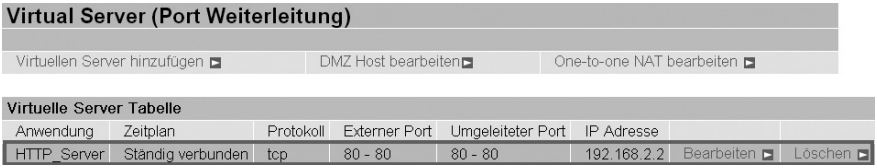
Die Port Nummer welche vom lokalen Server im LAN verwendet wird.

Interne IP Adresse:

Die private IP Adresse im LAN, auf welcher die Anwendung für den Virtuellen Server vorhanden ist. Aktive PC listet alle existierenden PCs in Ihrem Netzwerk auf.

Beispiel:
Jederzeitiger Router-Zugriff per Fernwartung

Wenn Sie z.B. jederzeit auf Ihren Router per Fernwartung mittels Web/HTTP zugriff haben wollen, müssen Sie den Port 80 (Web/HTTP) aktivieren und auf die IP Adresse des Routers umleiten. Dann werden alle eingehenden HTTP Anfragen zu dem Router mit der IP Adresse 192.168.2.1 weitergeleitet. Da der Port 80 schon zur Auswahl steht, müssen Sie nur neben **Anwendung** auf **Assistent** klicken. Ein Fenster mit voreingestellten Regeln erscheint und Sie müssen nur **HTTP_Server** auswählen.
Anwendung: HTTP_Server
Zeitplan: Ständig verbunden
Protokoll: tcp
Externer Port: 80-80
Umgeleiteter Port: 80-80
IP Adresse: 192.168.2.1



Bearbeiten:

Klicken Sie hier wenn Sie diesen Eintrag bearbeiten möchten.

Löschen:

Klicken Sie hier wenn Sie diesen Eintrag löschen möchten.

Die Port Weiterleitung birgt auch Sicherheitsrisiken, da außenstehende Benutzer die Möglichkeit haben sich mit Ihrem Netzwerk zu verbinden. Daher empfehlen wir nur die Ports zu öffnen, welche Sie für die jeweilige Anwendung benötigen. Tragen Sie nicht einfach einen Rechner als DMZ Host ein.

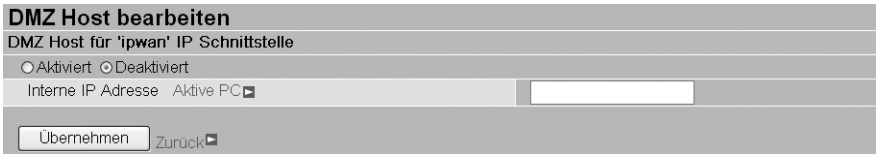
Wenn Sie NAT unter WAN Verbindung deaktiviert haben sind die Einstellungen im Bereich Virtueller Server ungültig.

Wenn Sie DHCP Server aktiviert haben, achten Sie darauf dass die IP Adressen für die Virtuellen Server außerhalb des IP-Bereiches des DHCP Servers liegen. Verwenden Sie für die Virtuellen Server statische IP-Adressen. Diese müssen aber im gleichen Subnetz liegen wie die IP Adresse des Routers.

DMZ Host bearbeiten

Der DMZ Host ist ein lokaler Computer der offen im Internet ist. Wenn Sie eine spezielle interne IP Adresse als DMZ Host festlegen, werden alle hereinkommenden Pakete von der Firewall und dem NAT Algorithmus überprüft und dann an den DMZ Host weitergeleitet, solange es keinen Konflikt mit einer anderen Portnummer des virtuellen Servers besteht.

Vorsicht: Der lokale Computer, welcher als DMZ Host festgelegt wird, kann ein Sicherheitsrisko darstellen.



- **Deaktiviert:** Die Funktion DMZ ist werksseitig deaktiviert.
- **Aktiviert:** Aktiviert die Funktion DMZ.

Interne IP Adresse:

Tragen Sie die statische IP Adresse für den DMZ Host ein wenn Sie DMZ **Aktiviert** haben. Bedenken Sie dass diese IP Adresse vor dem WAN/Internet ungeschützt ist.

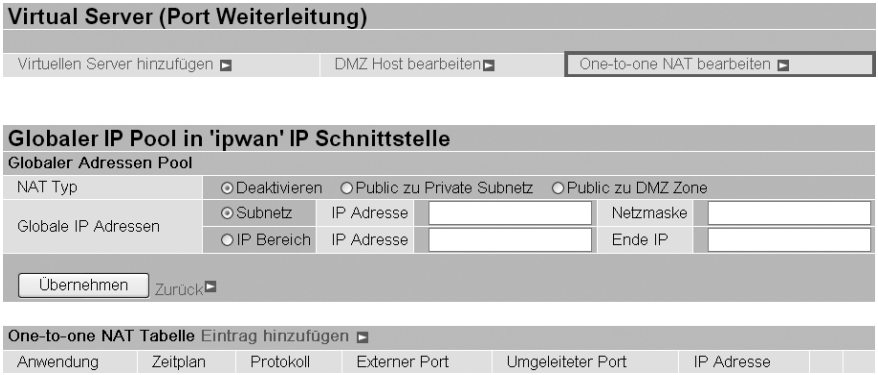
Aktive PC listet alle existierenden PCs in Ihrem Netzwerk auf.

Klicken Sie auf **Übernehmen** damit die Einstellungen wirksam werden.

One-to-One NAT (Network Address Translation) bearbeiten

One-to-One NAT verbindet eine spezifische private/lokale IP Adresse mit einer globalen/öffentlichen IP Adresse.

Wenn Sie mehrere öffentliche WAN IP Adressen von Ihrem ISP (Internet-Service-Provider) erhalten, erfüllen Sie die Voraussetzung One-to-One NAT mit diesen IP Adressen zu nutzen.



NAT Typ:

Wählen Sie den gewünschten NAT Typ. Die Funktion One-to-one NAT ist werksseitig deaktiviert.

Globale IP Adressen:

- **Subnetz:** Das Subnetz der öffentlichen WAN IP Adresse welche Sie von Ihrem ISP erhalten haben. Wenn Sie diese Information von Ihrem ISP erhalten haben, so tragen Sie diese hier ein. Andernfalls wählen Sie die Option IP Bereich.

- **IP Bereich:** Der IP Adressen Bereich Ihrer öffentlichen WAN IP Adressen. Z.B., IP: 192.168.2.1, Ende IP: 192.168.2.10

Klicken Sie auf **Übernehmen** damit die Einstellungen wirksam werden.

Klicken Sie auf Eintrag hinzufügen für eine neue One-to-One NAT Regel.

Zeitplan:

Hier können Sie einen selbst definierten Zeitplan für die Aktivierung Ihres Virtuellen Servers angeben. Wählen Sie den Zeitplan aus oder Ständig verbunden für den Virtuellen Server. Für die Einstellungen und weitere Information zum Zeitplan sehen Sie im Abschnitt Zeitplan nach.

Anwendung:

Tragen Sie hier einen Namen für die Anwendung ein oder klicken Sie auf Assistent um einen vorgegebene Anwendung auszuwählen.

Assistent :

20 vorgegebene Regeln haben Sie zur Auswahl. Wählen Sie eine Anwedung aus werden die Anwendung, das Protokoll sowie die externen und umgeleiteten Ports in die entsprechenden Felder übernommen.

Protokoll:

Das für den Virtuellen Server zu verwendende Protokoll. Zusätzlich zu dem benötigten Port müssen Sie auch das benötigte Protokoll angeben. Welches Protokoll wird von der Anwendung festgelegt. Die meisten Anwendungen verwenden TCP oder UDP.

Globale IP:

Geben Sie die öffentliche WAN IP Adresse für diese Anwendung an. Diese globale IP Adresse muss als **Globale IP Adresse** eingetragen sein.

Externer Port Aktive PC

Die Port Nummer welche auf der Remote/WAN Seite für den Virtuellen Server verwendet wird.

Umgeleiteter Port:

Die Port Nummer welche vom lokalen Server im LAN verwendet wird.

Interne IP Adresse:

Die private IP Adresse im LAN, auf welcher die Anwendung für den Virtuellen Server vorhanden ist. listet alle existierenden PCs in Ihrem Netzwerk auf.

Beispiele: Liste einiger Well-Known und registrierten Port Nummern.

Die Internet Assigned Numbers Authority (IANA) ist ein zentraler Koordinator für die Zuweisung der einzigartigen Parameterwerte für die Internet Protokolle. Port Nummern gehen von 0 bis 65535, aber nur Portnummern von 0 bis 1023 sind für privilegierte Services bestimmt und werden als “Well-Known Ports” bezeichnet. Die registrierten Ports sind von 1024 bis 49151 nummeriert. Die restlichen Ports werden als dynamische Ports oder private Ports bezeichnet, gehen von 49152 bis 65535.

Beispiele von Well-Known und registrierten Portnummern finden Sie unten, für weitere Informationen schauen Sie bitte auf http://www.iana.org/assignments/port-numbers nach.

Tabelle 5: Well-Known und registrierte Ports

Port Nummer	Protokoll	Beschreibung
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Zeitplan

Der Zeitplan unterstützt bis zu 16 Zeit Fenster welche Ihnen für Ihre Internetverbindung zur Verfügung stehen. In jedem Zeitprofil können Sie den Zeitplan anhand von Tag(en) und Zeiten festlegen, damit z.B. von Montags bis Samstags nur bestimmte Anwender oder Applikationen das Internet verwenden dürfen.

Der Zeitplan arbeitet in Verbindung mit der Zeit des Routers. Da der Router selbst keine Echtzeituhr integriert hat, bezieht er die Zeit mittels Simple Network Time Protocol (SNTP) von einem SNTP Server im Internet. Schauen Sie im Abschnitt **Zeitzone** für weitere Informationen nach. Die Zeit des Routers muss mit Ihrer lokalen Zeit übereinstimmen. Wenn die Zeit nicht übereinstimmt wird die Funktion Zeitplan nicht einwandfrei funktionieren (Zeitverschiebungen).

Zeitplan

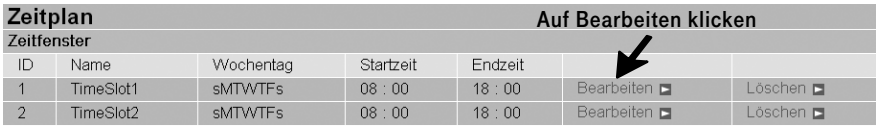
Zeitfenster

ID	Name	Wochentag	Startzeit	Endzeit		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen

Konfiguration des Zeitplan

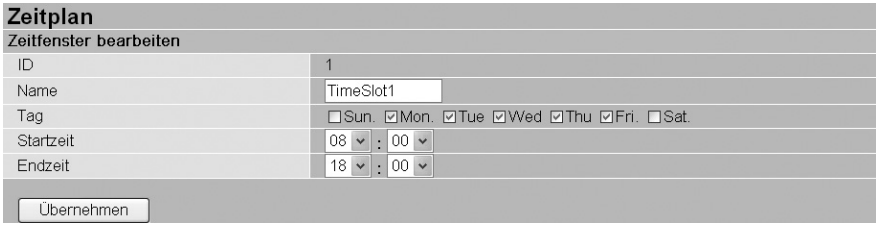
Zeitfenster bearbeiten

1. Wählen Sie ein Zeitfenster (Time Slot 1 bis 16) aus um es zu bearbeiten, klicken Sie auf **Bearbeiten.**


Zeitplan
Auf Bearbeiten klicken
Zeitfenster
ID Name Wochentag Startzeit Endzeit
1 TimeSlot1 sMTWTFs 08 : 00 18 : 00 Bearbeiten Löschen
2 TimeSlot2 sMTWTFs 08 : 00 18 : 00 Bearbeiten Löschen

Hinweis: Die Tage welche selektiert wurden, werden in Großbuchstaben angegeben. Tage in Kleinbuchstaben wurden nicht selektiert und dementsprechend wird die Regel auch nicht an diesen Tagen angewendet.

2. Die detaillierten Einstellungen des Zeitfensters werden angezeigt.



ID:

Die ID des Zeitfenster.

Name:

Hier können Sie einen Namen für das Zeitfenster eintragen.

Tag:

Werksseitig sind die Tage von Montag bis Freitag selektiert. Sie können selber die Tage festlegen, an welchen die Regel angewendet werden soll.

Startzeit:

Werksseitig ist 8:00 eingestellt. Sie können die Startzeit selber festlegen.

Endzeit:

Werksseitig ist 18:00 eingestellt. Sie können die Endzeit selber festlegen.

3. Klicken Sie auf **Übernehmen** damit die Einstellungen wirksam werden.

Löschen eines Zeitfenster

Klicken Sie auf **Löschen** damit das entsprechende Zeitfenster gelöscht wird. Die Tage werden alle deaktiviert.

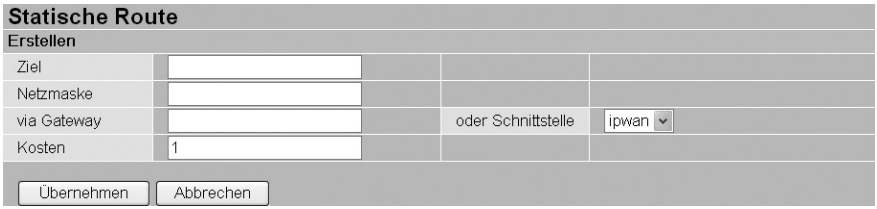
Erweitert

Die Konfiguration innerhalb dem Menü **Erweitert** sind für Anwender welche die hier angebotenen Funktionen benötigen. Nicht erfahrene Anwender sollten diese Funktionen und deren Einstellungen nicht verändern.

Es gibt sechs Unterpunkte im Menü **Erweitert. Statische Route, Dynamischer DNS, Prüfe Email, Geräte Management, IGMP** und **VLAN Bridge.**

Statische Route

Klicken Sie auf **Erstellen** um eine Statische Route hinzuzufügen.



Ziel:

Tragen Sie die Ziel IP Adresse ein.

Netzmaske:

Tragen sie die Netzmaske zu der Ziel IP Adresse ein

Gateway:

Tragen Sie die Gateway IP Adresse über welche die Pakete weitergeleitet werden sollen ein.

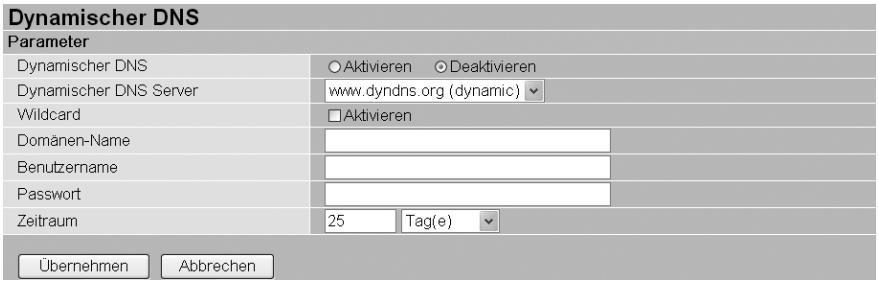
Schnittstelle:

Geben Sie die Schnittstelle an über welche die Pakete weitergeleitet werden sollen.

Kosten:

Auch Hop genannt. Normalerweise wird die 1 übernommen.

Dynamischer DNS



Die Dynamische DNS Funktion erlaubt Ihnen, einen Alias für eine dynamische IP Adresse als einen statischen Hostname darzustellen, indem Sie einen Domainnamen dazu nutzen. Dies ist besonders nützlich, wenn Sie einen Server über Ihre ADSL Verbindung hosten, so das jeder der sich mit dem Server verbinden will, einfach Ihren Domainnamen nutzt, anstelle der sich regelmäßig wechselnden IP Adresse. Diese dynamische IP Adresse ist die WAN IP des Routers, welche Ihnen von Ihrem ISP zugewiesen wird.

Zuerst müssen Sie sich bei einem Dynamischen DNS Provider registrieren und einen Account einrichten, z.B. bei http://www.dyndns.org//

Es werden mehr als 10 DDNS Dienste unterstützt.

- **Deaktivieren:** Klicken um die Funktion Dynamischer DNS zu deaktivieren.

- **Aktivieren:** Klicken um die Funktion Dynamischer DNS zu aktivieren. Die folgenden Felder müssen die notwendigen Informationen beinhalten, ansonsten wird die Funktion Dynamischer DNS wieder deaktiviert.

Dynamischer DNS Server:

Wählen Sie den DDNS Dienst bei welchem Sie einen Account haben.

Wildcard:

Wenn Wildcard aktiviert wird, kann z.B. die Homepage xyz.dyndns.org auch über Aliase erreicht werden. Dies kann hilfreich sein, wenn für die Homepage weitere Sub-Domains angelegt werden, z.B. support.xyz.dyndns.org oder guestbook.xyz.dyndns.org.

Domänen Name, Benutzername und Passwort:

Tragen Sie den registrierten Domänennamen sowie den dazugehörigen Benutzernamen und das Passwort ein.

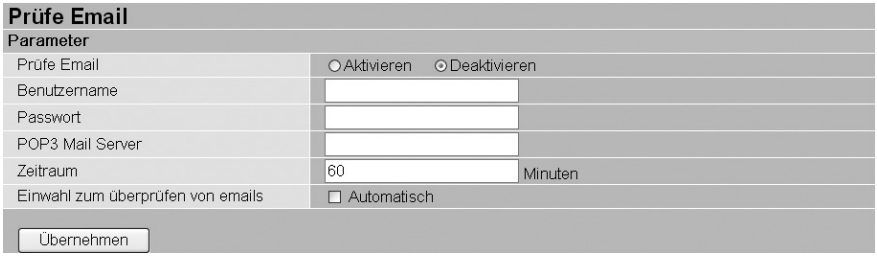
Zeitraum:

Geben Sie den Zeitraum an, wann der Router mit dem DDNS Server die erforderlichen Informationen austauschen soll. Unabhängig von dieser Einstellung, teilt der Router dem DDNS Server die IP Adresse mit sobald diese vom ISP geändert wurde.

Via WAN Schnittstelle:

Auswahl über welche WAN Schnittstelle Sie die DDNS Anfrage heraussenden wollen.

Prüfe Email



Diese Funktion erlaubt es Ihnen, über den Router Ihr POP3 Postfach nach neuen E-Mails zu überprüfen. Sie können den Status überprüfen im Abschnitt Status – E-Mail Status des Webinterfaces, welches zusätzlich genauere Informationen über die Anzahl der neuen E-Mails bereithält. Schauen Sie im Abschnitt Status dieser Anleitung für weitere Informationen nach.

- **Deaktivieren:** Klicken um die Funktion Prüfe Email zu deaktivieren.
- **Aktivieren:** Klicken um die Funktion Prüfe Email zu aktivieren. Die folgenden Felder müssen die notwendigen Informationen beinhalten:

Benutzername:

Tragen Sie den den Login-Namen des POP3 Accounts ein welchen Sie überprüfen wollen. Normalerweise ist die der text vor dem @ Symbol. Sollten Sie Probleme mit dem Login Account haben, kontaktieren Sie Ihren Provider.

Passwort:

Tragen Sie das Passwort des Email Accounts ein.

POP3 Mail Server:

Tragen Sie den Namen des (POP) Mail Server ein. Ihr Internet Service Provider wird Ihnen den Namen des POP Mail Server mitteilen.

Zeitraum:

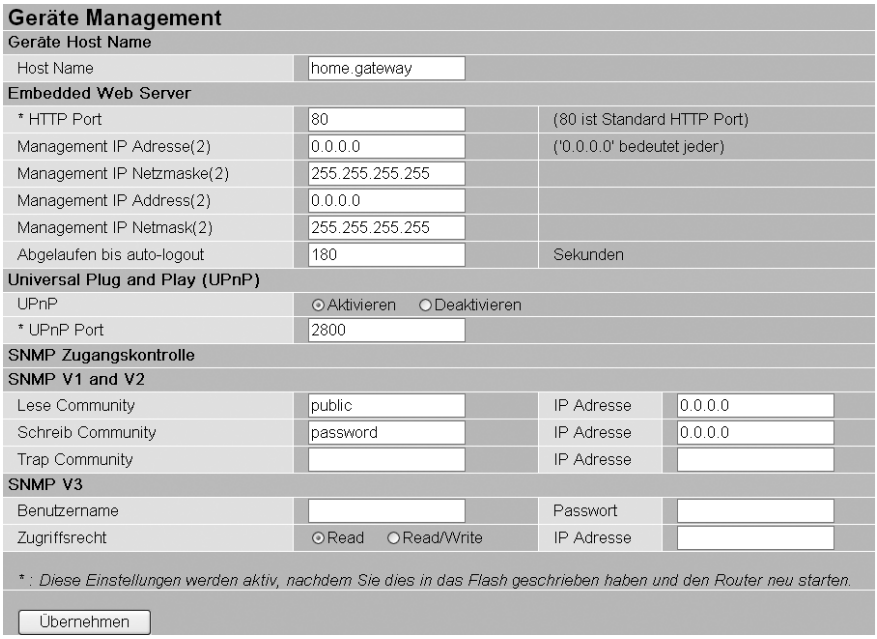
Tragen Sie den Intervall (Minuten) für die Prüfung des Email Accounts ein.

Einwahl zum überprüfen von Emails:

Wenn diese Funktion aktiviert ist, wird Ihr ADSL Router automatisch eine Verbindung ins Internet aufbauen, um zu prüfen, ob neue E-Mails vorhanden sind. Seien Sie bitte vorsichtig, wenn Ihre ADSL Nutzung über einen Zeittarif abgerechnet wird.

Geräte Management

Die Geräte Management Konfigurationseinstellungen erlauben Ihnen die Sicherheitsoptionen und Überwachungsfunktionen des Routers einzustellen.



Eingebauter Web Server

HTTP Port:

Dies ist der Port des integrierten Webservers (für Web-basierende Konfiguration) der benutzt wird. Der Standardwert ist der HTTP Port 80. Benutzer können einen alternativen Port festlegen, wenn Sie zum Beispiel einen zusätzlichen Webserver auf Ihrem PC laufen lassen.

Management IP Adresse:

Sie können die IP Adresse angeben, von der ein Log-in gestattet ist und die auf den Web Server des Routers zugreifen kann. Wenn Sie die IP Adresse als 0.0.0.0 festlegen, kann jeder Benutzer Sie sich von jeder IP Adresse einloggen.

Abgelaufen bis auto-logout:

Gibt den Zeitrahmen an bis zum automatischen Ausloggen des Benutzers.

Beispiel:
Benutzer A ändert die HTTP Port Nummer auf **100,** angegeben durch die eigene IP Adresse **192.168.2.55,** und gibt die auto-logout Zeit mit **100** Sekunden an. Der Router wird nur Benutzer A von der IP Adresse 192.168.2.55 zugriff auf das Web GUI über: **http://192.168.2.1:100** erlauben. Nach 100 Sekunden wird der Router Benutzer A automatisch ausloggen.

Universal Plug and Play (UPnP)

UPnP bietet Peer-to-Peer Netzwerkanschlussfähigkeit für PCs und andere Netzwerkgeräte an. Es erleichtert die Konfiguration unterschiedlicher Programme und den Datentransfer zwischen den Geräten. UPnP bietet viele Vorzüge für Nutzer von NAT Router über UPnP NAT Traversal und erleichtert die Arbeit für Port Forwarding mit unterstützten Systemen sehr, da die benutzten Programme dies automatisch kontrollieren und konfigurieren. Dadurch entfällt die zusätzliche Konfigurationsarbeit des Benutzers.

Das Betriebssystem und das relevante Programm müssen UPnP neben dem Router unterstützen. Windows XP und Windows ME unterstützen UPnP (wenn die Komponente schon installiert ist) von Anfang an, und Windows 98 Benutzer müssen die Internet Verbindungsfreigabe von Windows XP installieren, um UPnP zu unterstützen. Windows 2000 unterstützt kein UPnP.

- **Deaktivieren:** Klicken Sie hier, um die UPnP Funktion des Routers zu deaktivieren.

- **Aktivieren:** Klicken Sie hier, um die UPnP Funktion des Routers zu aktivieren.

UPnP Port:

Der Standardwert ist 2800. Es wird empfohlen diesen Standardwert zu nutzen. Wenn dieser Port mit anderen einem anderen benutzen Port einen Konflikt verursacht, so ändern Sie diesen Port.

SNMP Zugangskontrolle

(Entsprechende Software auf einem PC im gleichen LAN wird vorausgesetzt, um diese Funktion zu nutzen) – Simple Network Management Protocol.

SNMP V1 und V2:

Lese Community: Gibt einen Namen und eine IP Adresse an, die als Read Community identifiziert wird. Dieser Community String wird gegenüber dem String im Konfigurationsfile verglichen. Sobald der String richtig ist, können sich Benutzer die Daten ansehen.

Schreib Community: Gibt einen Namen und eine IP Adresse an, die als Write Community identifiziert wird. Dieser Community String wird gegenüber dem String im Konfigurationsfile verglichen. Sobald der String richtig ist, können sich Benutzer die Daten ansehen und modifizieren.

Trap Community: Gibt einen Namen und eine IP Adresse an, die als Trap Community identifiziert wird. Dieser Community String wird gegenüber dem String im Konfigurationsfile verglichen. Sobald der String richtig ist, werden die SNMP Traps an diese IP Adresse gesendet.

SNMP V3:

Spezifiziert Name und Passwort für die Authentifizierung und definiert die Zugriffsrechte von einer überprüfen IP Adresse. Nachdem die Autorisierung erfolgreich war, können Benutzer mit dieser IP Adresse Daten ansehen und modifizieren.

SNMP Version: SNMPv2c und SNMPv3

SNMPv2c kombiniert die gemeinschaftlich-basierende Annäherung von SNMPv1 mit dem Protokoll-Funktionen von SNMPv2, läßt dabei aber alle Sicherheits-Mechanismen von SNMPv2 weg. Das ”c” stammt von der Tatsache dass SNMPv2c den SNMPv1 Community String für die “Sicherheit” verwendet. SNMPv2c ist weit verbreitet und akzeptiert.
SNMPv3 beinhaltet starke Authentifizierungs-Mechanismen, mit Berechtigungen für Fern-Überwachung.
Unterstützte Traps: Cold Start, Authentication Failure.
Folgende MIBs werden unterstützt:

- **Vom RFC 1213 (MIB-II):**

  ☑ System group

- ☑ Interfaces group
- ☑ Address Translation group
- ☑ IP group
- ☑ ICMP group
- ☑ TCP group
- ☑ UDP group
- ☒ EGP (not applicable)
- ☑ Transmission
- ☑ SNMP group

- Vom RFC1650 (EtherLike-MIB):
  - ☑ dot3Stats
- Vom RFC 1493 (Bridge MIB):
  - ☑ dot1dBase group
  - ☑ dot1dTp group
  - ☑ dot1dStp group (konfiguriert als spanning tree)
- Vom RFC 1471 (PPP/LCP MIB):
  - ☑ pppLink group
  - ☒ pppLqr group
- Vom RFC 1472 (PPP/Security MIB):
  - ☑ PPP Security Group)
- Vom RFC 1473 (PPP/IP MIB):

☑ PPP IP Group

- Vom RFC 1474 (PPP/Bridge MIB):

  ☑ PPP Bridge Group

- Vom RFC1573 (IfMIB):

  ☑ ifMIBObjects Group

- Vom RFC1695 (atmMIB):

  ☑ atmMIBObjects

- Vom RFC 1907 (SNMPv2):

  ☑ only snmpSetSerialNo OID

IGMP

IGMP, bekannt als Internet Group Management Protocol, dient zur Organisation von Multicast Gruppen.

IGMP Weiterleitung:
Akzeptiere Multicast Pakete. Werkseinstellung **Aktiviert.**

IGMP Snooping:
Erlaube dem Switched Ethernet die Weiterleitung zu überprüfen und zu entscheiden. Werkseinstellung **Deaktiviert.**

VLAN Bridge

Dieser Abschnitt erlaubt Ihnen eine VLAN Gruppe zu erstellen und die Mitglieder zu spezifizieren.

VLAN Bridge

Parameter

Name	VLAN ID	Tagged Ports	UnTagged Ports	Bearbeiten	Löschen
DefaultVlan	1	Kein	ethernet,ipwan,	Bearbeiten	

VLAN erstellen

Bearbeiten:

Bearbeiten Sie die Mitglieder Ports in der ausgewählten VLAN Gruppe.

VLAN erstellen:

Erstellen Sie eine andere VLAN Gruppe.

Beispiele für erweiterte VLAN Einstellungen (Triply Play)

VLAN_Data:

Ethernet Port 1, Wireless und Wireless WDS sind für das Internet reserviert
- Ethernet Port 1 benötigt VC 0/40 Bridged.

VLAN_Video:

Ethernet Ports: 2 und 3:
- 0/33 Bi-direktional IP
- 0/34 Video
- 0/35 Video
- 0/36 Video Subscriber Services (EPG, EAS, etc.)
- 0/37 Video
- 0/38 Video
- 0/39 Spare

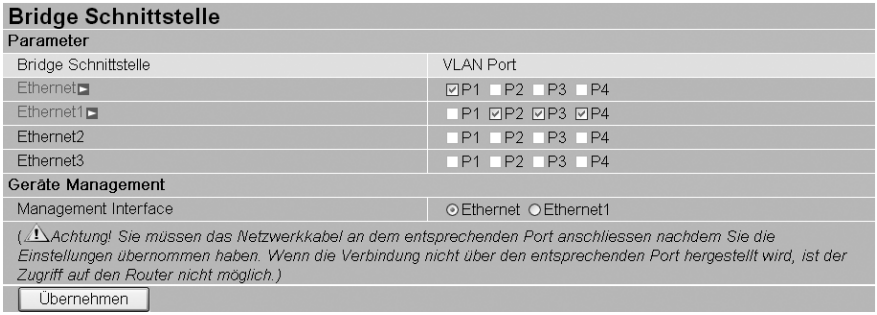
Schritt 1: Einstellungen Mitglieder Ports

Gehen Sie nach **Konfiguration ? LAN ? Bridge Schnittstelle.**

Sie können unter Bridge Schnittstelle für jede VLAN Gruppe Mitglieder Ports wählen. Im Beispiel werden zwei VLAN Gruppen erstellt.
Ethernet: P1 (Port 1)
Ethernet1: P2 und P3 (Port 2, 3) Bitte deaktivieren Sie zuerst P2, P3 vom Ethernet VLAN und aktivieren diese dann unter Ethernet1.

Hinweis: Sie sollten jede VLAN Gruppe behutsam einstellen. Jede Bridge Schnittstelle ist wie folgt zugeordnet.

Bridge Schnittstelle	VLAN Port (Startet immer mit)
Ethernet	P1 / P2 / P3
Ethernet1	P2 / P3
Ethernet2	P3


Bridge Schnittstelle
Parameter
Bridge Schnittstelle
VLAN Port
Ethernet
P1 P2 P3 P4
Ethernet1
P1 P2 P3 P4
Ethernet2
P1 P2 P3 P4
Ethernet3
P1 P2 P3 P4
Geräte Management
Management Interface
Ethernet Ethernet1
(Achtung! Sie müssen das Netzwerkkabel an dem entsprechenden Port anschliessen nachdem Sie die Einstellungen übernommen haben. Wenn die Verbindung nicht über den entsprechenden Port hergestellt wird, ist der Zugriff auf den Router nicht möglich.)
Übernehmen

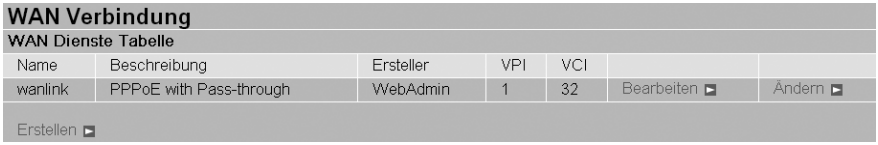
Schritt 2: Erstellen der WAN Schnittstelle

Gehen Sie nach **Konfiguration → WAN → ISP**

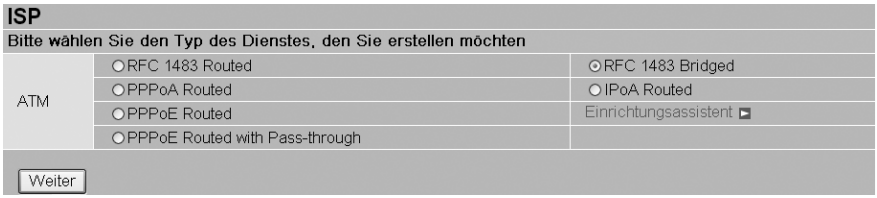
Wanlink ist die werksseitig eingestellte WAN Schnittstelle für Daten/Internet Dienste. Wenn Ihr ISP dieses Protokoll verwendet, klicken Sie auf **Bearbeiten** um weitere Parameter einzugeben, sofern nötig. Wenn Ihr ISP PPPoE nicht verwendet, so können Sie die werksseitige WAN Verbindung über **Ändern** wechseln.

In dem Beispiel wird 1/32 für Data/Internet und PPPoE verwendet; Klicken Sie auf **Bearbeiten** um die Einstellungen VPI/VCI auf 1/32 zu setzen.

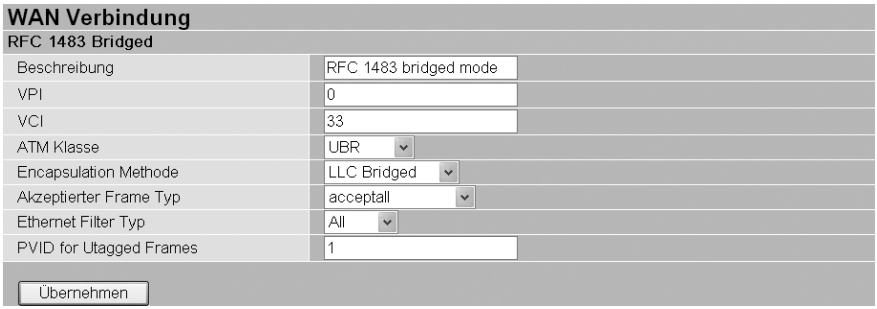
Klicken Sie auf **Erstellen** um eine weitere WAN Schnittstelle für Video Anwendungen einzurichten. Im Ganzen werden 8 VLANs unterstützt, daher können maximal 8 WAN Schnittstellen erstellt werden.



Im Beispiel weisen wir PVC 0/33 bis 0/39 unter Verwendung vom 1483 Bridged Mode zu für die Video Anwendung zu. Aktivieren Sie **RFC 1483 Bridged** und klicken Sie auf **Weiter** um die Einrichtung fortzusetzen.



Tragen Sie für VPI 0 und VCI 33 ein. Wählen Sie die ATM Klasse, Encapsulation Methode, Akzeptierter Frame Typ, Filter Typ und PVID für Untagged Frames.



VPI und VCI:

Tragen Sie die Informationen Ihres ISP ein.

ATM Klasse:

Der Quality of Service Ihres ATM Layers.

Encapsulation Methode:

Wählen Sie das Encapsulation Format, dies wird Ihnen von Ihrem ISP mitgeteilt.

Akzeptierter Frame Typ:

Geben Sie an welche Art von Datenverkehr diese Verbindung passieren soll, jeder Datenverkehr oder nur VLAN tagged Daten.

Filter Typ:

Geben Sie an welcher Ethernet Filter Typ für diese Bridge Schnittstelle angewendet werden soll.

Filter Typ	
All	Erlaubt allen Ethernet Paket Typen diesen Port zu verwenden.
Ip	Erlaubt nur IP/ARP Ethernet Paket Typen diesen Port zu verwenden.
Pppoe	Erlaubt nur PPPoE Ethernet Paket Typen diesen Port zu verwenden.

PVID für Untagged Frames:

PVID ist bekannt als Port VLAN Identifier. Wenn ein nicht markiertes (untagged) Paket vom eingehenden Port(s) empfangen wird diese Paket markiert (tagged) mit der angegebenen PVID.

Im Beispiel müssen Sie nur VPI und VCI wie angegeben ändern (0/33) – lassen Sie die anderen Einstellungen wie sie waren. Wiederholen sie diese Schritte indem Sie auf **Erstellen** ➜ dann **RFC1483 Bridged** wählen ➜ bis Sie von 0/34 bis 0/39 die Bridge Schnittstellen erstellt haben.

WAN Verbindung

WAN Dienste Tabelle

Name	Beschreibung	Ersteller	VPI	VCI		
wanlink	PPPoE Routed	WebAdmin	1	32	Bearbeiten	Ändern
rfc1483-0	RFC 1483 bridged mode	WebAdmin	0	33	Bearbeiten	Löschen
rfc1483-1	RFC 1483 bridged mode	WebAdmin	0	34	Bearbeiten	Löschen
rfc1483-2	RFC 1483 bridged mode	WebAdmin	0	35	Bearbeiten	Löschen
rfc1483-3	RFC 1483 bridged mode	WebAdmin	0	36	Bearbeiten	Löschen
rfc1483-4	RFC 1483 bridged mode	WebAdmin	0	37	Bearbeiten	Löschen
rfc1483-5	RFC 1483 bridged mode	WebAdmin	0	38	Bearbeiten	Löschen
rfc1483-6	RFC 1483 bridged mode	WebAdmin	0	39	Bearbeiten	Löschen

Schritt 3: VLAN Dienste einrichten

Gehen Sie nach **Konfiguration ➜ Erweitert ➜ VLAN Bridge**

DefaultVlan listet alle Mitglieder Ports auf. Es ist notwendig dass Sie für jedes VLAN die Mitglieder Ports gruppieren.
Im Beispiel werden zwei VLAN Gruppen benötigt: Data und Video.

Klicken Sie auf **VLAN erstellen** um eine weitere VLAN Gruppe einzurichten.

VLAN Bridge

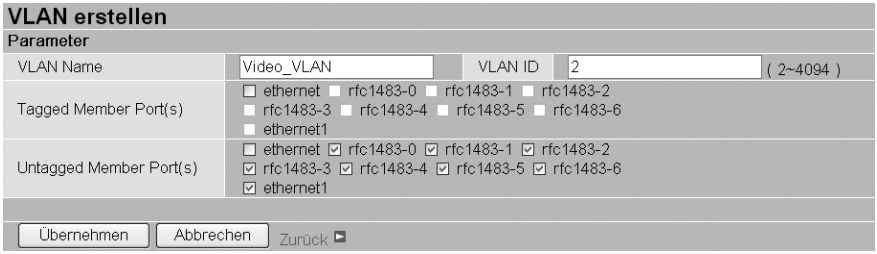
Parameter

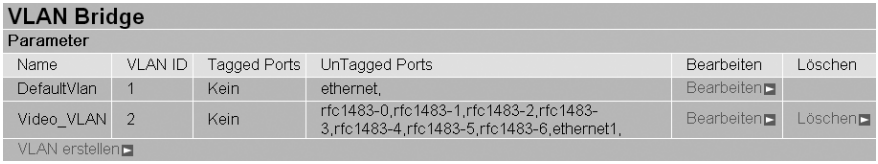
Name	VLAN ID	Tagged Ports	UnTagged Ports	Bearbeiten	Löschen
DefaultVlan	1	Kein	ethernet,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Bearbeiten	

VLAN erstellen

Geben Sie einen Namen und eine ID (PVID) an, damit die Video Gruppe identifiziert wird. Der gültig Bereich für PVID ist 1 bis 4094.

Beispiel:
VLAN untagged Ports für Data/Internet: ethernet, wireless and wireless_wds.
VLAN untagged Ports für Video: ethernet1, rfc-1483-0 - rfc-1483-6.
Klicken Sie auf **Übernehmen** damit die Einstellungen sofort wirksam werden.





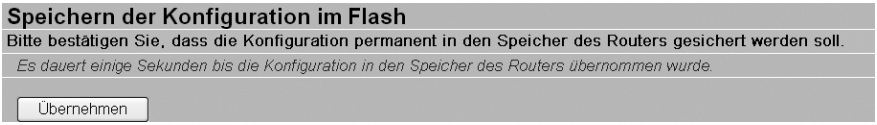
Nachdem Sie die **VLAN Bridge** und die **Bridge Schnittstelle** wie im Schritt 1 erstellt und verbunden haben, sehen Sie das konforme Verhältnis in diesem Fenster.

Schritt 4: IGMP Snooping Aktivieren

Gehen Sie nach **Konfiguration ➔ Erweitert ➔ IGMP.**
IGMP Snooping muss aktiviert damit der Video Stream korrekt weitergeleitet wird.

Speichern der Konfiguration im Flash

Nachdem Sie die Einstellungen des Routers verändert haben, müssen Sie alle Konfigurationsparameter im FLASH speichern, um einen Datenverlust zu verhindern, wenn der Router ausgeschaltet oder ein Reset durchgeführt wird. Klicken Sie auf **Speichern der Konfiguration im Flash** und dann auf **Übernehmen** um die neue Konfiguration im Flash zu speichern.


Speichern der Konfiguration im Flash
Bitte bestätigen Sie, dass die Konfiguration permanent in den Speicher des Routers gesichert werden soll.
Es dauert einige Sekunden bis die Konfiguration in den Speicher des Routers übernommen wurde.
Übernehmen

Ausloggen

Um das Web Interface des Routers zu verlassen, wählen Sie **Ausloggen.** Versichern Sie sich, daß Sie die Konfiguration gespeichert haben, bevor Sie ausloggen.

Bedenken Sie, daß der Router sich nur von einem PC gleichzeitig konfigurieren läßt. Sobald ein PC auf den Router zugreift, kann kein anderer einen Zugriff darauf erhalten, solange der PC sich nicht ausgeloggt hat. Wenn der vorherige PC sich vergisst auszuloggen, so kann der zweite PC nach einer vorgegeben Zeit – Standardwert ist 3 Minuten - auf den Router zugreifen. Sie können diesen Wert modifizieren im Abschnitt **Erweitert – Geräte Management** des Web Interface. Schauen Sie im Abschnitt **Erweitert** in dieser Anleitung nach für weitere Informationen zu diesem Thema.

Ratgeber

Weiterführende Hinweise

Der Ratgeber enthält weiterführende Hinweise zu folgenden Themen:

- Was bei der Verkabelung zu beachten ist
- Auslieferzustand

Was bei der Verkabelung zu beachten ist

Die Verkabelung des Speedports 400P kann problemlos verlängert werden. Kabel in passender Länge können Sie im Computerfachhandel kaufen. Bedenken Sie, dass die Leitungsqualität mit Vergrößerung des Abstandes von der Vermittlungsstelle abnehmen kann.

Beachten Sie beim Kauf der Kabel die folgenden Hinweise:

	Maximale Länge	Kabeleingenschaften
Netzwerkkabel	100 m	Netzwerkkabel 10bT, 1.1 verdrahtet, STP
DSL-Kabel	20 m	Netzwerkkabel 10bT, 1.1 verdrahtet, UTP
ISDN-Kabel	10 m	Netzwerkkabel 10bT, 1.1 verdrahtet, UTP

Auslieferzustand

Merkmal	Beschreibung
IP Adresse:	192.168.2.1
Subnet Maske:	255.255.255.0
Benutzername:	admin
Passwort:	admin
DHCP Server:	Aktiviert
DHCP Start IP Adresse:	192.168.2.100
IP Adressen Pool:	100
Firewall:	Aktiv mit der Einstellung „Niedrige Sicherheitsstufe“

Problembehandlung

Bevor Sie sich an den Technischen Kundendienst wenden, versuchen Sie bitte zunächst bei einer eventuellen Störung eine Behebung an Hand der folgenden Tabelle.

Fehler beim Öffnen der Benutzeroberfläche

LAN-Verbindung

Sie haben den Speedport 400P über eine LAN-Verbindung an einen Computer angeschlossen und die IP-Einstellungen in dem Speedport 400P entsprechend den vorgegebenen Werkseinstellungen. Beim Versuch, die Benutzeroberfläche zu öffnen, erhalten Sie jedoch eine Fehlermeldung. Überprüfen Sie bitte folgende Punkte:

- Stellen Sie sicher, dass alle Kabelverbindungen fest stecken.
- Die IP-Adressen der angeschlossenen Computer müssen automatisch zugewiesen werden.
- Geben Sie im Internetbrowser als Adresse statt „home.gateway“ folgende IP-Adresse ein:
  192.168.2.1

IP-Einstellungen prüfen

Voraussetzung für diese Überprüfung ist, dass die IP-Einstellungen in dem Speedport 400P den vorgegebenen Werkseinstellungen entsprechen.

Stellen Sie sicher, dass der Computer seine IP-Adresse automatisch vom DHCP-Server des Speedport 400P bezieht. Wie Sie diese Einstellung überprüfen und gegebenenfalls ändern, wird im Abschnitt „DHCP Server“ ab Seite 41 beschrieben.

IP-Einstellungen

Der Speedport 400P verfügt über einen eigenen DHCP-Server. Das bedeutet, dass den angeschlossenen Computern ihre IP-Adresse vom Speedport 400P zugewiesen wird. Die angeschlossen Computer müssen dafür so eingerichtet

sein, dass sie ihre IP-Adresse vom Speedport 400P automatisch beziehen können. Die Schritte zur Überprüfung und Einstellung dieser Option unterscheiden sich in den verschiedenen Betriebssystemen. Lesen Sie dazu den Abschnitt für Ihr Betriebssystem ab Seite 11.

Wenn der Speedport 400P in einem Netzwerk betrieben wird, dann darf in diesem Netzwerk kein anderer DHCP-Server aktiviert sein.

Probleme beim Starten des Speedport 400P

Problem	Maßnahme
Die LED's sind aus, obwohl das Gerät angeschaltet ist.	Überprüfen Sie die Kabelverbindung zwischen dem Adapter und dem Router. Wenn der Fehler weiterhin besteht, liegt es möglicherweise an der Hardware. In diesem Fall wenden Sie sich bitte an den technischen Support.
Sie haben Ihr Router Login und/oder Passwort vergessen.	Versuchen Sie den Standardlogin und Passwort admin/admin. Wenn dies fehlschlägt so drücken Sie den Resetknopf auf der Rückseite für mehr als 6 Sekunden um die Werkeinstellungen wiederherzustellen.

Problem mit der WAN Schnittstelle

Problem	Maßnahme
Initialisierung der PVC-Verbindung schlägt fehl. Keine Synchronisation.	Vergewissern Sie sich, daß das Kabel zwischen dem ADSL-Port und dem Splitter intakt ist. Die LED's an der Frontseite des Routers für ADSL sollten leuchten. Überprüfen Sie, ob VPI, VCI und die Encapsulation-Einstellungen identisch mit denen sind, die Sie vom Telefonanbieter bzw. vom ISP haben. Starten Sie den Router neu. Sollte das Problem weiterhin bestehen, ist es ratsam, die oben genannten Daten mit denen Ihres Telefonanbieters bzw. Ihres ISPs zu vergleichen.
Regelmäßiger Verlust der ADSL Leitungssynchronisation	Überprüfen Sie, ob alle anderen Geräte an der gleichen Leitung wie Ihr Speedport 400P Router einen Splitter vorgeschaltet haben. Überprüfen Sie ob der Splitter korrekt arbeitet und installiert ist. Falsche oder fehlerhafte Splitter können dazu führen, dass Ihr Speedport 400P Router regelmäßig die ADSL Leitungssynchronisation verliert.

Problem mit der LAN Schnittstelle

Problem	Maßnahme
Das Gerät kann keine Station im LAN anpingen.	Überprüfen Sie die LED für Ethernet an der Frontseite des Routers. Die LED sollte für einen Port leuchten, an dem eine Workstation angeschlossen ist. Sollte diese aus ein, überprüfen Sie die Verkabelung zwischen dem Gerät und der Workstation. Vergewissern Sie sich, daß die IP-Adresse und die Teilnetz-Maske zwischen dem Gerät und den Workstations übereinstimmen.

Anhang

Technischer Kundendienst

Bei der Arbeit mit dem Speedport 400P werden sicherlich auch einmal Fragen auftauchen. In diesem Kapitel erhalten Sie Hinweise auf Informationsquellen, die Sie bei der täglichen Arbeit mit dem Speedport 400P unterstützen. Über das Internet erhalten Sie weitere Informationen, Produktbeschreibungen und Updates.

Informationen und Updates

Informationen zum Speedport 400P finden Sie hier:

- Installation und Inbetriebnahme

Über das Internet hält die Deutsche Telekom Antworten auf häufig gestellte Fragen zu Ihren Produkten bereit. Dort können Sie auch neuesten Software-Updates herunterladen. Rufen Sie die folgende Adresse auf:

www.telekom.de/faq

Unterstützung durch den Support

Tipp

Bitte nutzen Sie zuerst die oben beschriebenen Informationsquellen, bevor Sie den Support anrufen!

Bei technischen Problemen mit Ihrem Speedport 400P können Sie sich während der üblichen Geschäftszeiten an die Service-Hotline 0180 / 5 1990 wenden. Der Verbindungspreis bei einem Anruf aus dem Festnetz der Deutschen Telekom AG beträgt 0,12 € pro angefangene 60 Sekunden.

Bereiten Sie folgende Informationen für Ihren Berater vor:

- Welches Betriebssystem verwenden Sie (z.B. Windows XP oder Windows ME)?
- Mit welcher Firmware arbeitet der Speedport 400P. Die Firmware-Version finden Sie in der Benutzeroberfläche des Speedport 400P.

- Vermuten Sie eine Störung Ihres Anschlusses, wenden Sie sich bitte an den Service Ihres Netzbetreibers. Für den Netzbetreiber Deutsche Telekom AG steht Ihnen der T-Service unter freecall 0800/3302000 zur Verfügung.

Für allgemeine Fragen zu DSL und Ihrem T-DSL- oder T-Net-Anschluss wenden Sie sich bitte an Ihren T-Punkt oder die Kundenberatung unter freecall 0800/3301000.

Gewährleistung für Speedport 400P

Der Händler, bei dem das Gerät erworben wurde (Deutsche Telekom AG oder Fachhändler), leistet für Material und Herstellung des Telekommunikationsendgerätes eine Gewährleistung von 2 Jahren ab der Übergabe.

Dem Käufer steht im Mangelfall zunächst nur das Recht auf Nacherfüllung zu. Die Nacherfüllung beinhaltet entweder die Nachbesserung oder die Lieferung eines Ersatzproduktes. Ausgetauschte Geräte oder Teile gehen in das Eigentum des Fachhändlers über.

Bei Fehlschlagen der Nacherfüllung kann der Käufer entweder Minderung des Kaufpreises verlangen oder von dem Vertrag zurücktreten und, sofern der Mangel von dem Händler zu vertreten ist, Schadensersatz oder Ersatz vergeblicher Aufwendungen verlangen.
Der Käufer hat festgestellte Mängel dem Händler unverzüglich mitzuteilen. Der Nachweis des Gewährleistungsanspruchs ist durch eine ordnungsgemäße Kaufbestätigung (Kaufbeleg, ggf. Rechnung) zu erbringen.
Schäden, die durch unsachgemäße Behandlung, Bedienung, Aufbewahrung, sowie durch höhere Gewalt oder sonstige äußere Einflüsse entstehen, fallen nicht unter die Gewährleistung, ferner nicht der Verbrauch von Verbrauchsgütern, wie z. B. Druckerpatronen und wiederaufladbare Akkumulatoren.

Vermuten Sie einen Gewährleistungsfall mit Ihrem Telekommunikationsendgerät, können Sie sich während der üblichen Geschäftszeiten an die T-Service-Hotline 0180 / 5 1990 wenden. Der Verbindungspreis beträgt 0,12€ pro angefangene 60 Sekunden bei einem Anruf aus dem Festnetz der Deutschen Telekom. Erfahrene Techniker beraten Sie und stimmen mit Ihnen das weitere Vorgehen ab.

Technische Daten

- Abmessungen: ca. 232mm x 152mm x 38mm
- Netzspannung für das Steckernetzteil: 230 Volt / 50 Hertz
- Leistungsaufnahme im Leerlauf: ca. 4,6 Watt
- Maximale Leistungsaufnahme im Betrieb: ca. 5,9 Watt
- Zulässige Umgebungstemperaturen im Betriebsfall: +5°C bis +40°C
- Zulassung: Dieses Gerät ist für die Verwendung in Deutschland bestimmt.

Reinigen

Wischen Sie den Speedport 400P von Zeit zu Zeit mit einem leicht feuchten, fusselfreien Tuch oder mit einem Antistatiktuch ab, niemals mit einem trockenen Tuch (wegen statischer Aufladung).
Vermeiden Sie bitte den Einsatz von Putz- und Scheuermitteln.

CE-Konformitätserklärung

Dieses Gerät erfüllt die Anforderungen der EU-Richtlinie:

1999/5/EG Richtlinie über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität.
Die Konformität mit der o. a. Richtlinie wird durch das CE-Zeichen bestätigt.
Die Konformitätserklärung kann unter folgender Adresse eingesehen werden:

Deutsche Telekom AG
T-Com Zentrale
CE Management
Postfach 1227
48542 Steinfurt

Recycling

Hat Ihr Speedport 400P ausgedient, bringen Sie das Altgerät zur Sammelstelle Ihres kommunalen Entsorgungsträgers (z. B. Wertstoffhof). Das nebenstehende Symbol bedeutet, dass das Altgerät getrennt vom Hausmüll zu entsorgen ist. Nach dem Elektro- und Elektronikgerätegesetz sind Besitzer von Altgeräten gesetzlich gehalten, alte Elektro- und Elektronikgeräte einer getrennten Abfallerfassung zuzuführen. Helfen Sie bitte mit und leisten Sie einen Beitrag zum Umweltschutz, indem Sie das Altgerät nicht in den Hausmüll geben.

Ihr Gerät enthält geheime Daten, deren Bekanntgabe Ihnen zum Schaden gereichen kann. Wollen Sie das Gerät z. B. entsorgen oder weitergeben, setzen Sie das Gerät zurück auf Werkseinstellungen.

Rücknahme von CD-ROM

Ihre nicht mehr benötigte Produkt-CD-ROM nimmt die Deutsche Telekom AG in den T-Punkten kostenlos zurück und führt sie der Wiederverwertung zu.

Stichwortverzeichnis

A

Anhang 177
CE-Konformitätserklärung 179
Gewährleistung für Speedport 400P 178
Informationen und Updates 177
Recycling 180
Reinigen 179
Rücknahme von CD-ROM 180
Technische Daten 179
Technischer Kundendienst 177
Unterstützung durch den Support . 177
Anschluss von einem oder mehreren Computern 1
Ausloggen 172

D

Dynamischer DNS 159

E

Einrichtungsassistent . . . . . 19 , 38
Anderer Anbieter 46
Ausloggen 20
Im Internet surfen 21
T-DSL Business mit dynamischer IP Adresse 40
T-DSL Business mit fester IP Adresse 43
Erstkonfiguration 15
Der Web-Konfigurator 15
Konfiguration mit dem Einrichtungsassistent 16
Erweiterte Konfiguration 23
ARP Tabelle 27
DHCP Tabelle 29
Diagnose 36
Email Status 34
Ereignis Protokoll 34
Fehler Protokoll 35
Fristablauf Tabelle 30
IPSec Status 32
L2TP Status 33
Leased Tabelle 30
NAT Sitzungen 35
Permanent Tabelle 30
PPTP Status 31
Routing Tabelle 28
Status 24
UPnP Portmap 37

F

Firewall und Zugangskontrolle 86
Firewall Protokoll 102
Generelle Einstellungen 87
Paket Filter 89
URL Filter 99

G

Gerät in Betrieb nehmen 3
Anschließen 5
Anschlüsse auf der Rückseite des Speedport 400P 5
Anzeigen 6
Aufstellen des Speedport 400P 4
Aufstellungsort 4
Gerät auspacken 3
ISDN-Anschluss (optional) 9
Speedport 400P am DSL anschließen 8
Speedport 400P an die Stromversorgung anschließen 7
Speedport 400P mit dem LAN Anschluss des Computers verbinden . 8
Verpackungsinhalt überprüfen 3
Wandmontage 4
Geräte Management 162
Eingebauter Web Server 162
SNMP V1 und V2 164
SNMP V3 164
SNMP Version 164
Universal Plug and Play (UPnP) . . . 163

I

IGMP 166
Internetverbindung für alle Computer . . . 1
IPSec 108
Erweiterte Optionen 110
Konfiguration einer IPSec VPN Verbindung 108
ISDN Einwahl 136

K

Konfiguration 50
LAN (Local Area Network) 51
WAN (Wide Area Network) 58
Konfiguration des Speedport 400P . . . 10
Konfiguration des PCs unter Windows 2000 13
Konfiguration des PCs unter Windows XP 11
Prüfen der Netzanbindung der Ethernetkarte 10
Vorbereiten des einzubindenden Rechners/Netzwerkes 10

L

L2TP 112
LAN zu LAN L2TP Verbindung 116
Remote Zugriffs L2TP Verbindung . 113
LAN (Local Area Network) 51
Bridge Schnittstelle 51
DHCP Server 56
Ethernet 52
Ethernet Client Filter 52
Port Einstellungen 54

P

Paket Filter 89
Angriffserkennung 96
Hacker Attack Typen 98

Konfiguration Paket Filter 94
Paket Filter – Raw IP Filter hinzufügen 92
Paket Filter –TCP/UDP Filter hinzufügen 91
Voreingestellte Paket Filter Regeln . . 89
PPTP 103
LAN zu LAN PPTP Verbindung . . . 105
PPTP Remote Zugriffs Verbindung . 103
Problembehandlung 174
Fehler beim Öffnen der Benutzeroberfläche 174
Problem mit der LAN Schnittstelle . 176
Problem mit der WAN Schnittstelle . 176
Probleme beim Starten des Speedport 400P 175
Prüfe Email 160

Q

QoS (Quality of Service) 137
IP Throttling ausgehend (LAN zum WAN) 140
IP Throttling eingehend (WAN zum LAN) 142
Priorisation 137

R

Ratgeber 173
Auslieferzustand 173
Was bei der Verkabelung zu beachten ist 173

S

Schutz durch integrierte Firewall 2
Speichern der Konfiguration im Flash . 172
Statische Route 158
System 81
Benutzer Verwaltung 84
Firmware Upgrade 82
Neustart 84
Remote Zugriff 82
Sichern / Wiederherstellen 83
Zeitzone 81

V

Virtual Server (“Port Forwarding”) . . . 147
DMZ Host bearbeiten 150
One-to-One NAT (Network Address Translation) bearbeiten 152
Virtuellen Server hinzufügen 148
VLAN Bridge 166
VPN (Virtual Private Networks) 103
Beispiele VPN Konfiguration 119
IPSec 108
L2TP 112
PPTP 103
VPN Verbindung
IPSec Host-to-LAN VPN Verbindung 127
IPSec LAN-zu-LAN 124
IPSec VPN im Hauptbüro . . . 125 , 127
L2TP VPN im Hauptbüro . . . . 129 , 133
IPSec VPN in der Filiale 126
L2TP im Filialbüro 134
L2TP VPN im Firmenbüro 131

LAN-zu-LAN L2TP VPN Verbindung 132

Remote Access L2TP VPN Dial-in Verbindung 128

Remote Access L2TP VPN Dial-out Verbindung 130

Routers zur Einwahl in den Server . 132

W

WAN (Wide Area Network) 58

ADSL 78

Backup ISP 76

DNS 77

ISP 58

Z

Zeitplan 155

Konfiguration des Zeitplan 155

Bei Fragen erreichen Sie uns unter der Rufnummer
freecall 0800 33 07000.
Besuchen Sie uns im T-Punkt oder im Internet:
www.t-com.de

Herausgeber:

Deutsche Telekom AG
T-Com Zentrale
Postfach 2000
53105 Bonn

Stand: 16.06.2006
Änderungen und Irrturm vorbehalten
Printed in Taiwan
Papier chlorfrei gebleicht

CE